مكتب الأمم المتحدة
لمكافحة الإرهاب
مركز الأمم المتحدة لمكافحة الإرهاب

الإنتربول

بتمويل من
الاتحاد الأوروبي

أمن الفضاء الإلكتروني والتكنولوجيات الجديدة

دليل المستجيبين الأوائل لجمع الأجهزة الرقمية في ميدان المعركة

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.

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.

مكتب الأمم المتحدة لمكافحة الإرهاب

مقر الأمم المتحدة

نيويورك، نيويورك 10017

www.un.org/counterterrorism/ar

200، رصيف شارل ديغول

69006 ليون، فرنسا

www.interpol.int/en

المحتويات

توطئة مشتركة

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

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

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

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

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

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

ستيفن كافانا
المدير التنفيذي
للخدمات الشرطية في الإنتربول

شكر وتقدير

أُعدت هذه الوثيقة من خلال المساهمات وراجعتها مجموعة واسعة من أصحاب المصلحة. وعلى وجه التحديد، يود مكتب الأمم المتحدة لمكافحة الإرهاب الاعتراف بالمساهمة التي قدمها كل من:

- **السيدة سيسيليا ناديو** – مسؤولة قانونية ومنسقة العدالة الجنائية، المديرية التنفيذية لمكافحة الإرهاب
- **السيد وينثروب ويلز** – مدير البرنامج، المعهد الدولي للعدالة وسيادة القانون
- **السيدة ماري بولوس** – ضابط أركان، قسم التحديات الأمنية الطارئة، قسم مكافحة الإرهاب، حلف الناتو
- **السيد أدريان فينكارت** – خبير الأدلة الجنائية الرقمية، يونيتاد

مصطلحات وتعاريف

الذكاء الاصطناعي	من المفهوم عموماً أن هذا المصطلح يشير إلى مجالٍ يهتم بتطوير أدواتٍ تكنولوجيةٍ تمارس صفاتٍ بشرية مثل التخطيط والتعلم والاستدلال والتحليل.
ميدان المعركة	يشير مصطلح ميدان المعركة لأغراض هذه الوثيقة إلى وصف البيئة التي تجري فيها إجراءات مكافحة الإرهاب والتي قد يكون فيها الأفراد العسكريون أول المستجيبين بسبب الجوانب غير الخاضعة للحكم أو التي تتسم بفقدان الإدارة في المنطقة. ولأغراض هذه الوثيقة، يوضح استخدام ميدان المعركة الفرق بين مسرح الجريمة العادي والظروف الخاصة التي يحتاج المستجيبون الأوائل إلى العمل في ظلها وتعديل أنشطتهم بما يتماشى مع تفويضهم الأصلي. ولا يهدف استخدام مصطلح "ميدان المعركة" في هذه الوثيقة إلى التأثير على أي تعريفات تستخدمها المنظمات والتشريعات الوطنية أو الإقليمية.
سلسلة العهدة	هي سجلات زمنية عن كيفية الاستيلاء على الأدلة والتعامل معها. ويجب أن يتضمن أي سجل على الأقل المعلومات المستولى عليها ومتى ومن قام بالتعامل مع المعلومات ومتى نُقلت إلى جهات إنفاذ القانون أو المحكمة[1].

1 المبادئ التوجيهية للمديرية التنفيذية للجنة مكافحة الإرهاب لتيسير الاستخدام والمقبولية كدليل في المحاكم الجنائية الوطنية للمعلومات التي يجمعها الجيش ويعالجها ويحفظها ويشاركها لمقاضاة الجرائم الإرهابية (2019). https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/cted_military_evidence_guidelines.pdf.

إجراءات العدالة الجنائية	عملية قانونية لتوجيه اتهامات جنائية ضد فرد أو كيان، وإجراءات المحكمة وإصدار الأحكام وكذلك الإصلاحات وإعادة التأهيل.
الأجهزة الرقمية	الأجهزة الإلكترونية التي تخزن المعلومات أو تعالجها إلكترونياً. تشمل الأجهزة الرقمية، على سبيل المثال لا الحصر، الهواتف الذكية وأجهزة الكمبيوتر المحمولة والأجهزة اللوحية ومحركات الأقراص الصلبة الخارجية وأنظمة التخزين عن بُعد وأنظمة الطيران المسير والمعدات المحمولة على متن السفن. قد تحتوي الأجهزة الرقمية على أنواع مختلفة من المعلومات الإلكترونية كالمستندات والصور ومقاطع الفيديو والتسجيلات الصوتية ومعلومات النظام والسجلات وبيانات التعريف.
علم الأدلة الجنائية الرقمية	فرع من علوم الأدلة الجنائية يركز على تحديد المعلومات المخزنة إلكترونياً والحصول عليها ومعالجتها وتحليلها والإبلاغ عنها. ويتمثل الهدف الرئيسي لعلم الأدلة الجنائية الرقمية في استخراج البيانات من جهاز إلكتروني ومعالجتها لتصبح معلومات استخباراتية قابلة للتنفيذ، وتقديم النتائج للمحاكمة. تستخدم جميع العمليات تقنيات علم الأدلة الجنائية الرقمية السليمة لضمان قبول النتائج في المحكمة[2].
الأدلة الإلكترونية	"الدليل" هو مصطلح رسمي يدل على المعلومات التي تشكل جزءاً من المحاكمة، بمعنى أنها تستخدم لإثبات الجريمة المزعومة أو دحضها. كل الأدلة معلومات، لكن ليست كل المعلومات أدلة. وبالتالي تعتبر المعلومات الشكل الأصلي للأدلة[3]. أما الأدلة بشكلها الإلكتروني فهي أي معلومات مخزنة إلكترونياً يمكن استخدامها كدليل في المحكمة أو الإجراءات القانونية.
حقائب فاراداي	غلاف مصنوع من مادة موصّلة كالشبكة المعدنية لحجب المجالات الكهرومغناطيسية. وهذا يجعلها مثالية لحماية الأجهزة الإلكترونية من تداخل ترددات الراديو. وغالباً ما تُستخدم حقائب فاراداي لحماية الهواتف المحمولة وأجهزة الكمبيوتر المحمولة والأجهزة الحساسة الأخرى من الاختراق أو التتبع.
المستجيبون الأوائل	الأفراد أو المجموعات من الهيئات المعينة الذين يصلون إلى مكان الهجوم الإرهابي بعد موظفي الطوارئ أو معهم، وهم مخصصون لجمع الأجهزة الرقمية كجزء من مهمتهم في مكافحة الإرهاب. ولا ينطبق هذا المصطلح على موظفي الطوارئ كرجال الإطفاء والعاملين الصحيين. ولأغراض هذه الوثيقة، فالمستجيبين الأوائل هم أي موظفين عسكريين أو مدنيين تابعين لمنظمة حكومية وطنية أو إقليمية أو دولية يكونون أول من يصل إلى مسرح الجريمة الإرهابية والذين تسمح مهامهم بجمع الأجهزة الرقمية. كما يمكن أن يوجد موظفو المنظمات غير الحكومية في ميدان المعركة وأن يجمعوا الأجهزة الرقمية، لكنهم لا يعتبرون أول المستجيبين لأغراض هذه الوثيقة.
الاستخبارات	الناتج عن جمع المعلومات التي تم جمعها من مجموعة واسعة من المصادر وإعدادها ونشرها وتحليلها وتفسيرها، وذلك ليستنير بها صناع القرار لأغراض التخطيط لاتخاذ القرارات أو الإجراءات على المستوى الاستراتيجي أو التشغيلي أو التكتيكي. وينبغي جمع المعلومات الاستخبارية والاحتفاظ بها واستخدامها ومشاركتها بما يتوافق مع التزامات الدول الأعضاء ذات الصلة بموجب القانون الدولي لحقوق الإنسان.
التحقيقات الجنائية	عملية جمع المعلومات (أو الأدلة) لتحديد ما إذا كانت الجريمة قد ارتكبت، والتعرف على الجاني وتقديم الأدلة لدعم الادعاء في الإجراءات القانونية.

2 الإنتربول – الأدلة الجنائية الرقمية https://www.interpol.int/en/How-we-work/Innovation/Digital-forensics.

3 المبادئ التوجيهية للمديرية التنفيذية للجنة مكافحة الإرهاب لتيسير الاستخدام والمقبولية كدليل في المحاكم الجنائية الوطنية للمعلومات التي يجمعها الجيش ويعالجها ويحفظها ويشاركها لمقاضاة الجرائم الإرهابية (2019). https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/cted_military_evidence_guidelines.pdf.

إجراءات إنفاذ القانون	يصف هذا المصطلح عادة إجراءات إنفاذ القانون ضد التهديدات بناءً على السلطة القانونية والمتخذة حيال التهديد والتي قد تشمل احتجاز فرد أو أفراد وتعطيل أنشطة الجهة المهدِّدة (كإزالة المحتوى ومصادرة الأصول) وما إلى ذلك.
الفرز الميداني	لغرض هذه الوثيقة، عملية التقييم والقياس وتحديد أولويات الأجهزة الرقمية أو وسائط التخزين لإجراء مزيد من الفحص والتحليل عن طريق الوصول إلى المعلومات المخزنة على جهاز يعمل في الموقع والبحث عنها رقمياً، وذلك بغية نسخ المعلومات المهمة المخزنة عليه أو تحديد ما إذا كانت حاوية البيانات هذه ذات صلة بالتحقيق في مكافحة الإرهاب، دون النسخ الكامل لجميع البيانات المخزنة على الجهاز.
التكنولوجيات الجديدة	في حين أن مصطلح التكنولوجيات الجديدة يغطي مجموعة واسعة من التكنولوجيات المختلفة[4]، لأغراض هذه الوثيقة، تشير التكنولوجيات الجديدة إلى استخدام هذه التكنولوجيات الجديدة وإساءة استخدامها[5].
الملاحقة القانونية/ المقاضاة	عملية قانونية لتوجيه تهم الإرهاب ضد فرد أو كيان وجلسة المحكمة القانونية أو البت في القضية وإصدار الحكم بالإدانة.
إعادة التأهيل	في السياقات الجنائية، يُستخدم مصطلح "إعادة التأهيل" للإشارة إلى التدخلات التي يجريها نظام الإصلاحيات بهدف تغيير آراء الجاني أو سلوكه لتقليل احتمالية معاودة ارتكابه الجريمة، وكذلك إعداد الجاني ودعم إعادة إدماجه في المجتمع.
إعادة الإدماج	عملية شاملة لإدماج الشخص مرة أخرى في البيئة الاجتماعية أو الوظيفية أو كلاهما.
الفرز والتصنيف	عملية القياس والتقييم وتحديد أولويات الأجهزة الرقمية أو وسائط التخزين في الموقع ليصار إلى مزيد من الفحص والتحليل. وغالباً ما تكون هذه الخطوة الأولى في الموقع لتحقيقات الأدلة الجنائية الرقمية، وتساعد المحققين في العثور على حاويات البيانات ذات الصلة بسرعة. ولأغراض هذه الوثيقة، يتضمن الفرز تحديد الأجهزة الرقمية وتحديد أولوياتها في ميدان المعركة لجمعها بناءً على عوامل مثل قيمتها في تحقيقات مكافحة الإرهاب وقيمة البيانات المخزنة. وفي سياق هذا المستند، لا يتضمن الفرز العمليات المباشرة أو الوصول إلى البيانات الموجودة على الجهاز بواسطة المستجيبين الأوائل[6].
الإرهاب	الأفعال الإجرامية، ضد المدنيين أو غيرهم، المرتكبة بقصد التسبب في الوفاة أو الإصابة الجسدية الخطيرة، أو أخذ الرهائن، بغرض إثارة حالة من الرعب لدى عامة الناس أو في مجموعة من الأشخاص أو أشخاص معينين أو تخويف السكان أو إجبار حكومة ما أو منظمة دولية ما على أداء عمل معين أو الامتناع عنه، ويشكل جرائم تقع ضمن نطاق الاتفاقيات والبروتوكولات الدولية المتعلقة بالإرهاب وكما هي محددة فيها[7].
زيتابايت	زيتابايت واحد يساوي مليار تيرابايت.

4 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.

5 وثيقة مشروع التكنولوجيا لمكافحة الإرهاب – الملحق الأول: وصف الإجراء.

6 لمزيد من التفاصيل عن الفرز الميداني مع توفر بيانات الجهاز في الموقع، راجع مبادئ الإنتربول التوجيهية للمستجيبين الأوائل في الأدلة الجنائية الرقمية، آذار/مارس 2021، https://www.interpol.int%2Fcontent%2Fdownload%2F16243%2Ffile%2FGuidelines_to_Digital_Forensics_First_Responders_V7.pdf.
لمزيد من المعلومات عن تطور الفرز الرقمي، راجع بي كارير (2011)، الفرز الرقمي في الأدلة الجنائية الرقمية: دليل ميداني للمستجيبين الأوائل، سينجرس.

7 انظر قرار مجلس الأمن (2004) 1566 (2004), S/RES/1566، الفقرة 3.

ملخص تنفيذي

يتطلب ميدان المعركة من الأفراد العمل في بيئات معقدة ومتغيرة باستمرار. وغالباً ما تتميز ديناميكيات ميدان المعركة بالإلحاح والارتياب والفوضى ومستويات عالية من المخاطر. يتضح في ميدان المعركة الفرق بين مسرح الجريمة العادي والظروف الخاصة التي يعمل في ظلها المستجيبون الأوائل ويضبطون أنشطتهم بما يتماشى مع تفويضهم الأصلي. ولأغراض هذا التقرير، يُفهم المستجيبون الأوائل على أنهم أي موظفين عسكريين أو مدنيين تابعين لمنظمة حكومية وطنية أو إقليمية أو دولية، يكونون أول من يصل إلى مسرح الجريمة الإرهابية والذين يسمح تفويضهم بجمع الأجهزة الرقمية. يمكن أيضاً لموظفي الجمعيات الأهلية الحضور في ميدان المعركة وجمع الأجهزة الرقمية، لكنهم لا يعتبرون مستجيبين أوائل لغرض هذه الوثيقة.

تمثل مكافحة الإرهاب في ميدان المعركة للمستجيبين الأوائل مجموعة من التحديات البارزة. ويعد جمع الأجهزة الرقمية في ميدان المعركة لأغراض الأدلة أحد هذه التحديات الجديدة وغير المألوفة.

في حال افتقار المستجيبين الأوائل إلى المعرفة والوعي بالمخاطر والممارسات الجيدة في جمع الأجهزة الرقمية، قد تتسبب تصرفاتهم أثناء جمع الأجهزة الرقمية والتعامل معها في ميدان المعركة في ضرر محتمل لسلامتهم وسلامة الأشخاص الآخرين والمناطق المحيطة بهم، وقد تعرّض هذه التصرفات الإجراءات الجنائية لخطر جرائم إرهابية.

تهدف هذه الوثيقة إلى تقديم إرشادات عملية للمستجيبين الأوائل بشأن جمع الأجهزة الرقمية في ميدان المعركة لأغراض التحقيق في الجرائم الإرهابية ومحاكمتها والبت فيها. وتحدد الوثيقة الجوانب والمبادئ العملية والتكنولوجية التي يجب على المستجيبين الأوائل معرفتها والالتزام بها من أجل الحفاظ على سلامتهم وسلامة الآخرين وضمان سلامة الأجهزة الرقمية وموثوقيتها كأدلة.

تُبين الوثيقة الإجراءات التي يتعين على المستجيبين الأوائل اتخاذها في ميدان المعركة لضمان الحفاظ على سلامتهم وأمنهم وكذلك سلامة الآخرين وأمنهم، بالإضافة إلى التعامل مع الأجهزة الرقمية الموجودة في مكان الحادث وجمعها، واتخاذ الإجراءات المطلوبة قبل وصول الأجهزة إلى معمل الأدلة الجنائية الرقمية لاستغلالها بالشكل الأمثل، بطريقة تضمن قبول المعلومات والبيانات الموجودة في الأجهزة كدليل في الإجراءات الجنائية.

يستهدف هذا الدليل العملي المستجيبين الأوائل الذين لديهم معرفة أو خبرة محدودة للغاية في جمع الأجهزة الرقمية أو الأدلة الرقمية ولكنهم مكلفون بذلك في ميدان المعركة لأغراض مكافحة الإرهاب.

ويركز الدليل على أربع مراحل تتعلق بجمع الأجهزة الرقمية في ميدان المعركة لأغراض الإجراءات الجنائية: (1) الوصول إلى مكان الحادث و(2) فرز الأجهزة الرقمية و(3) جمع الأجهزة وتغليفها و(4) نقل الأجهزة خارج مسرح الأحداث.

الشكل 1

تقدم الوثيقة قائمة بالإجراءات المقترحة لكل مرحلة لمساعدة المستجيبين الأوائل، إلى جانب المواصفات والقوالب في الملحق.

[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)[8] 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)[9] ورقم 2396 (2017)[10] 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[11]، 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[12].

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

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

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

11 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).

12 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 2

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 تقديم إرشادات عملية للمستجيبين الأوائل بشأن جمع الأجهزة الرقمية في ميدان المعركة لأغراض التحقيق لاحقاً في الجرائم الإرهابية ومحاكمتها والبت فيها. وتحدد الوثيقة الجوانب والمبادئ العملية والتكنولوجية التي يجب على المستجيبين الأوائل معرفتها والالتزام بها في سبيل الحفاظ على سلامتهم وسلامة الآخرين وضمان سلامة الأجهزة الرقمية وموثوقيتها كدليل.

1 – 3 – 1 نطاق العمل

تبين الوثيقة الإجراءات التي يوصى المستجيبون الأوائل باتخاذها في ميدان المعركة لضمان ما يلي:

- الحفاظ على سلامتهم وأمنهم وكذلك سلامة الآخرين وأمنهم
- الكشف عن أي أجهزة رقمية متروكة في ميدان المعركة وجمعها بشكل مناسب

- التعامل مع أي أجهزة تم جمعها بشكل مناسب حتى وصولها إلى معمل الأدلة الجنائية الرقمية ليصار إلى استغلالها بالشكل الأمثل.

يتمثل الهدف العام في ضمان قبول المعلومات والبيانات الموجودة في الأجهزة كأدلة في الإجراءات الجنائية.

تم تناول الأطر القانونية المتعلقة باستخدام المعلومات التي تم جمعها في ميدان المعركة ومقبوليتها كأدلة في المحاكم الجنائية الوطنية للتحقيق في الجرائم الإرهابية في "المبادئ التوجيهية لتيسير استخدام المعلومات التي تم جمعها ومقبوليتها والتعامل معها وحفظها كدليل في المحاكم الجنائية الوطنية"[13]. ويجب تطويرها لتفي بجميع الشروط القانونية اللازمة، وينشرها الجيش لملاحقة الجرائم الإرهابية.

ليس الهدف من هذه الوثيقة أن يستخدمها المستجيبون الأوائل كدليل مرجعي لمنهجية علم الأدلة الجنائية الرقمية أو كإطار لمبادئ سلسلة العهدة. الهدف هو دعم المستجيبين الأوائل الذين ليس لديهم خبرة في جمع الأجهزة الرقمية والتعامل معها من خلال إرشادهم بكيفية جمع الأجهزة الرقمية ونقلها من ميدان المعركة إلى معمل الأدلة الجنائية الرقمية المخصص.

1 – 3 – 2 الجمهور المستهدف

يستهدف هذا الدليل العملي المستجيبين الأوائل، الذين ليس لديهم أي معرفة أو خبرة أو لديهم معرفة محدودة للغاية في جمع الأجهزة الرقمية أو الأدلة الرقمية ولكنهم مكلفون بذلك في ميدان المعركة لأغراض مكافحة الإرهاب.

يُنصح بشدة أن تتضمن فرق المستجيبين الأوائل متخصصين في الأدلة الجنائية الرقمية، لكن الوثيقة تتناول الفجوة المهنية والتكنولوجية التي تواجه العديد من الدول الأعضاء، وكذلك تستهدف جميع الموظفين الذين قد يكلفون بوظائف المستجيبين الأوائل وجمع الأجهزة الرقمية في ميدان المعركة.

1 – 3 – 3 الفوائد

تقدم هذه الوثيقة للمستجيبين الأوائل عملية واضحة ومنظمة يجب اتباعها لجمع الأجهزة الرقمية في ميدان المعركة لدعم التحقيق والملاحقة القضائية والبت في الجرائم الإرهابية ضمن سلسلة العدالة الجنائية. على وجه التحديد، يساعد هذا الدليل في تحسين مهارات المستجيبين الأوائل واستعدادهم من خلال تعريفهم بالمبادئ والمتطلبات الأساسية لجمع الأجهزة الرقمية لأغراض الأدلة، وفي الوقت نفسه تخفيف المخاطر المرتبطة بسلامة الموظفين وأمنهم. ومن خلال اتباع المبادئ التوجيهية، يمكن للمستجيبين الأوائل زيادة كفاءتهم وامتثالهم لمبادئ سلسلة العهدة، وزيادة مقبولية الأجهزة الرقمية والمعلومات الرقمية كدليل في إجراءات مكافحة الإرهاب، والملاحقة القضائية الناجحة للجرائم الإرهابية.

1 – 3 – 4 أوجه القصور

لا تقدم هذه الوثيقة إرشادات بشأن الجوانب القانونية المتعلقة بجمع الأجهزة الرقمية في ميدان المعركة. وتفترض الوثيقة أن المستجيبين الأوائل مستوفون جميع الشروط القانونية اللازمة ويتصرفون في ظل الاحترام الكامل لسيادة القانون. والمحكمة هي التي تحدد مقبولية أي دليل، ويشمل ذلك الأدلة (المحتملة) التي تُجمع من الأجهزة الرقمية الموجودة في ميدان المعركة.

13 المبادئ التوجيهية لتيسير الاستخدام والمقبولية كدليل في المحاكم الجنائية الوطنية للمعلومات التي يجمعها الجيش ويعالجها ويحفظها ويشاركها لمقاضاة الجرائم الإرهابية، والتي وضعتها المديرية التنفيذية للجنة مكافحة الإرهاب، 2019، cted_military_evidence_guidelines.pdf(un.org).

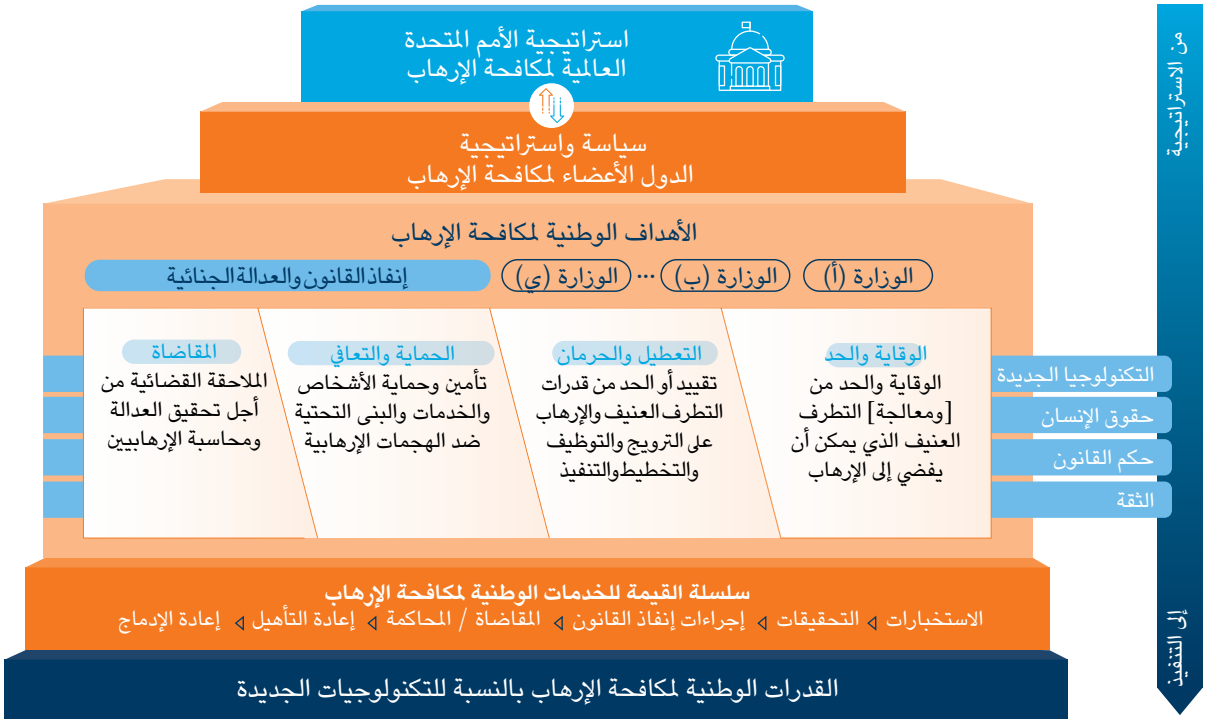
[ثانيا]
النهج

2 – 1 لمحة عامة

يسعى التقرير إلى دعم الدول الأعضاء وتمكينها من إيجاد مجموعة فعالة من الحلول لجمع الأجهزة الرقمية في ميدان المعركة بما يتماشى مع استراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب، ومع الاحترام الكامل لضوابط حقوق الإنسان وسيادة القانون.

2 – 2 الإطار التوجيهي

الشكل 3



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 لمكافحة الإرهاب

الوصف	الخدمات
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 4

أعدت هذه الوثيقة واستندت إلى مجموعة واسعة من المدخلات التي شملت وثائق مشروع تكنولوجيا مكافحة الإرهاب، ومشاورة أصحاب المصلحة، والتحليل الداخلي، والبحث المكتبي، واجتماعات فريق الخبراء، والتنسيق مع الكيانات المنخرطة في اتفاق الأمم المتحدة العالمي لتنسيق مكافحة الإرهاب، والإطار التوجيهي كما هو مبين أعلاه في القسم 2 – 2.

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

أُعد هذا الدليل مسترشداً بالأبحاث والمبادئ التوجيهية والمنشورات الحالية وآخذاً إياها في الاعتبار وبانياً عليها ومستكملاً إياها. وتتضمن هذه المصادر ما يلي:

الجدول 3 - المراجع

1	المبادئ التوجيهية لتيسير الاستخدام والمقبولية كدليل في المحاكم الجنائية الوطنية للمعلومات التي يجمعها الجيش ويعالجها ويحفظها ويشاركها لمقاضاة الجرائم الإرهابية، والتي وضعتها المديرية التنفيذية للجنة مكافحة الإرهاب ("المبادئ التوجيهية للأدلة العسكرية")، كانون الأول/ديسمبر 2019.
2	المنتدى العالمي لمكافحة الإرهاب، توصيات أبوجا بشأن جمع الأدلة واستخدامها ومشاركتها لأغراض الملاحقة الجنائية للإرهابيين المشتبه بهم، أيلول/سبتمبر 2018.
3	الإنتربول، المبادئ التوجيهية للمستجيبين الأوائل في مجال الأدلة الجنائية الرقمية، أفضل الممارسات للبحث عن الأدلة الإلكترونية والرقمية ومصادرتها، آذار/مارس 2021.
4	يوروجست، مذكرة بخصوص أدلة ميدان المعركة، أيلول/سبتمبر 2020.
5	يوروجست، دراسة حالة بخصوص مكافحة الإرهاب: رؤى 2020-2021، كانون الأول/ديسمبر 2021.
6	مجلس أوروبا، توصية اللجنة الوزارية للدول الأعضاء بشأن استخدام المعلومات المجمعة في مناطق النزاع كأدلة في الإجراءات الجنائية المتعلقة بالجرائم الإرهابية، 30 آذار/مارس 2022.
7	كريستيان براتشيني وتيمو فايسينن وميشيل سادلون وخير الدين باشي وأغوستينو بانيكو وكريس فان دير ميج وماريو هويس إنتفيلد في مركز إكسلنس للدفاع السيبراني التعاوني التابع لحلف شمال الأطلسي، الاستخبارات الرقمية وجمع الأدلة في ميدان المعركة، الاستخبارات الرقمية وجمع الأدلة في العمليات الخاصة، 2016.
8	وزارة الخارجية الأمريكية ووزارة العدل ووزارة الدفاع، المبادئ التوجيهية الأمريكية غير الملزمة بشأن استخدام أدلة ميدان المعركة في الإجراءات الجنائية المدنية.
9	أكاديمية جنيف للقانون الإنساني الدولي وحقوق الإنسان واللجنة الدولية للصليب الأحمر، المبادئ التوجيهية بشأن التحقيق في انتهاكات القانون الإنساني الدولي: القانون والسياسة والممارسات الجيدة، أيلول/سبتمبر 2019.

[ثالثا]
مقدمة

3 – 1 لمحة عامة

التقدم التكنولوجي آخذ في التسارع، وينتج عن ذلك ابتكارات يستغلها الإرهابيون يوماً بعد يوم لتعزيز أجنداتهم التدميرية. كما يشكل الانتشار السريع لمنصات الاتصال وشبكات التواصل الاجتماعي وتقنيات التشفير والتقنيات الناشئة تحديات كبيرة أمام هيئات إنفاذ القانون. وتزايد استخدام الإرهابيين للتكنولوجيا في الاتصالات والتجنيد والتخطيط، وجعل تلك البصمات الرقمية مصادر قيمة للمعلومات في الكشف عن أنشطتهم. ويتضمن علم الأدلة الجنائية الرقمية جمع الأدلة الرقمية وحفظها وتحليلها وعرضها بشكل منهجي، مما يسمح للمحققين بإعادة بناء الأحداث وتحديد الجناة وتفكيك الشبكات الإرهابية. ويسعى هذا الدليل إلى تقديم إرشادات حول جمع الأجهزة الرقمية والتعامل معها بطريقة تقلل من تعطيل هذه الأجهزة في حالتها الراهنة التي قد تحتوي على معلومات قيمة. ولا يقتصر هذا النهج الاستباقي على منع الهجمات الإرهابية، بل يدعم كذلك محاكمة الأفراد المتورطين في الأنشطة الإرهابية.

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 معزز يضاعف قدرات 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.

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.

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

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

إن التقدم في تكنولوجيا المعلومات والاتصالات وتوافرها جعلها مغرية للجماعات الإرهابية وجماعات التطرف العنيف لاستغلال الإنترنت ووسائل التواصل الاجتماعي في تيسير مجموعة واسعة من الأنشطة، بما في ذلك التحريض، والتطرف، والتجنيد، والتدريب، والتخطيط، وجمع المعلومات، والتواصل، والتحضير، والترويج، والتمويل. وتستغل الجماعات الإرهابية ببراعة أيضا عدم المساواة في النوع الاجتماعي 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. في الوقت ذاته، قد تعني التطورات في مجالات الذكاء الاصطناعي والتعلم الآلي والجيل الخامس من الاتصالات والروبوتات والبيانات الضخمة والمرشحات الخوارزمية والتكنولوجيا الحيوية والسيارات الذاتية 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.

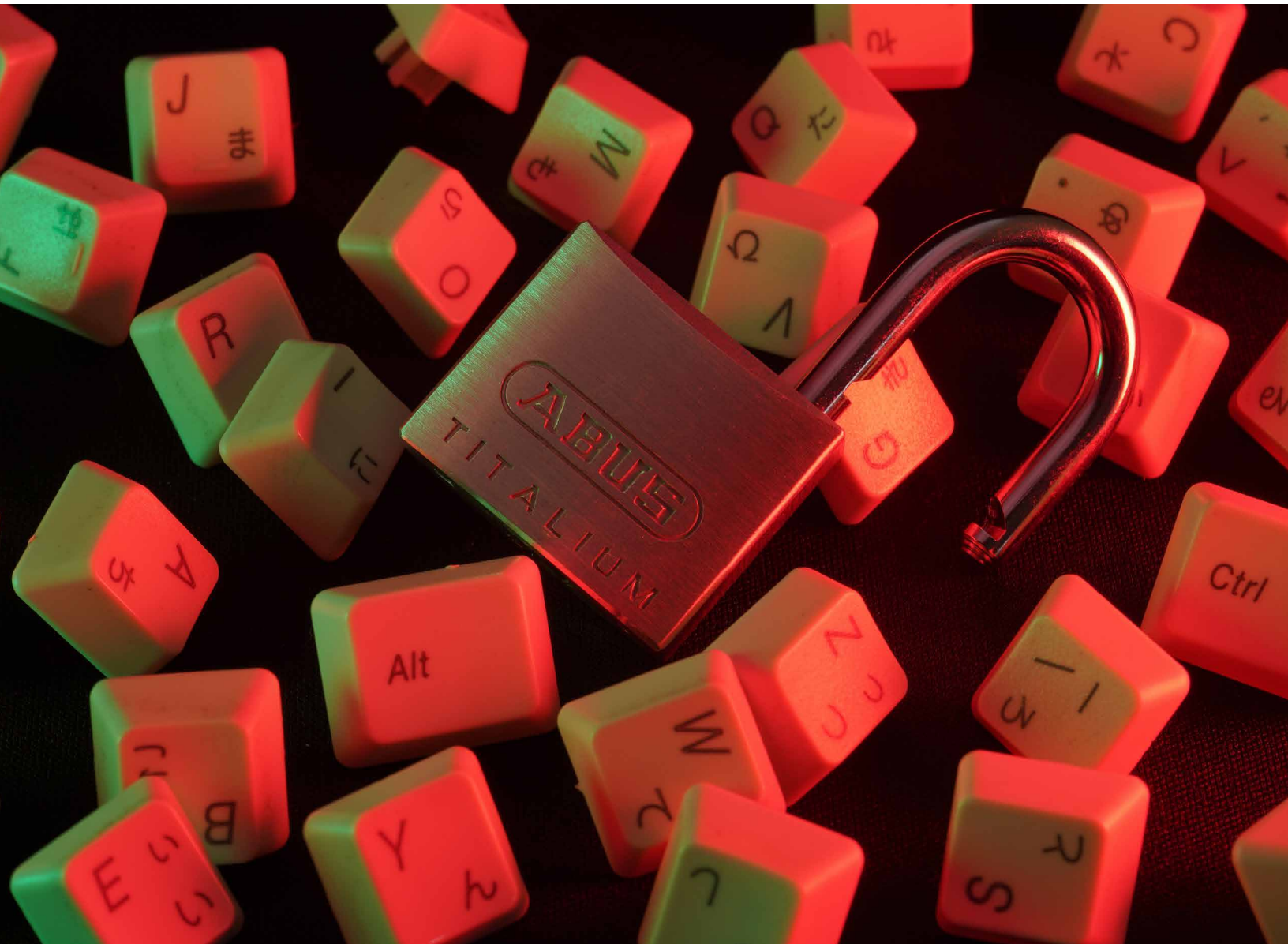
3 - 2 - 3 حقوق الإنسان والتكنولوجيات الجديدة

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 المحلي والمدني 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 مراراً وتكراراً على الارتباط المتبادل بين التكنولوجيات الجديدة ومكافحة الإرهاب وحقوق الإنسان، بما في ذلك المساواة في النوع الاجتماعي 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 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، ومراعاة حق حرية التعبير.



[رابعا]
جمع الأجهزة الرقمية في ميدان المعركة

4 – 1 لمحة عامة

يتحدث هذا الفصل عن مفهوم المعلومات الرقمية في ميدان المعركة ويقدم إرشادات عملية للمستجيبين الأوائل عن كيفية جمع الأجهزة الرقمية والتعامل معها في ميدان المعركة ونقلها إلى معمل الأدلة الجنائية الرقمية بطريقة تضمن سلامة المستجيبين الأوائل وأمن وسلامة الأشخاص الآخرين والمناطق المحيطة بها وأمنهم، فضلاً عن قيمة الأجهزة (والمعلومات المستمدة منها) كأدلة لاستخدامها المحتمل في الإجراءات الجنائية.

ويحتم استمرار تطور التكنولوجيا السريع على المستجيبين الأوائل أخذ التأثير المحتمل للتطورات الجديدة على الممارسات والإجراءات المقترحة في هذه الوثيقة في الحسبان عند تطبيق هذا الدليل.

ويركز الدليل على أربع مراحل تتعلق بجمع الأجهزة الرقمية في ميدان المعركة لأغراض الإجراءات الجنائية: (1) الوصول إلى مكان الحادث و(2) فرز الأجهزة الرقمية و(3) جمع الأجهزة وتغليفها و(4) نقل الأجهزة خارج مسرح الأحداث.

تتضمن كل مرحلة قائمة بالإجراءات المقترحة للمستجيبين الأوائل وتوصيف لهم:

- تكون الإجراءات المسبوقة بكلمة "**يجب**" في هذا الدليل إلزامية للمستجيبين الأوائل من أجل الحفاظ على القيمة الإثباتية للجهاز الرقمي أو عندما يلزم إكمال الإجراء قبل الانتقال إلى الإجراء التالي.
- تكون الإجراءات المسبوقة بكلمة "**ينبغي**" في هذا الدليل موصى بها وهي الممارسات الفضلى التي يجب أن يتبعها المستجيبون الأوائل للامتثال الكامل لمنهجيات علم الأدلة الجنائية الرقمية. وتجوز الاستثناءات عندما يكون الوقت اللازم لتنفيذ هذه الإجراءات قد يعرض المستجيبين الأوائل أو غيرهم من الموظفين للخطر.
- الإجراءات المذكورة إلى جانب عبارة "**إذا كان ذلك ممكناً**"، هي أفضل الممارسات المقترحة التي يجب أن يتبعها المستجيبون الأوائل ولكنها ليست إلزامية ولن تؤثر على مقبولية الأجهزة الرقمية كدليل في الإجراءات الجنائية.

يضمن اتباعُ توصيات هذا الدليل للمستجيبين الأوائل إمكانية استخدام الأجهزة الرقمية المجموعة من ميدان المعركة ومخرجاتها في الإجراءات الجنائية كأدلة.

يجب تنفيذ هذه الإرشادات وفقاً لبروتوكولات الأمن والسلامة التي يتبعها المستجيبون الأوائل. وفي حال اشتباه الفريق في وجود متفجرات أو أجهزة مفخخة في الموقع، يجب على الفريق الالتزام بالبروتوكول الخاص به فيما يتعلق بالإجراءات المتعلقة بالمواقع التي تنطوي على خطر الانفجار.

4 - 2 المعلومات الرقمية الخاصة بميدان المعركة

عاد الانتشار السريع للأجهزة الرقمية والتقدم في تكنولوجيا المعلومات والاتصالات على الإرهابيين والمنظمات الإرهابية بأدوات جديدة للتجنيد والتمويل والتدريب والتخطيط وتنفيذ الهجمات، ويشمل ذلك الهجمات السيبرانية. وكثيراً ما تترك هذه الإجراءات آثاراً رقمية على الأجهزة المستخدمة، وتوثق أنشطتها، ويشمل ذلك أنشطتها على الإنترنت وأنشطة الاتصال.

ويمكن أن تساعد المعلومات الرقمية في منع الأعمال الإرهابية والأنشطة الإرهابية وتحديد مرتكبيها والكشف عن الأدلة على أنشطتهم وتحديد داعميهم وتقديمهم إلى العدالة. ويستحسن أن تستخدم الدول الأعضاء المعلومات الرقمية التي تُجمع في ميدان المعركة كأدلة رقمية للتحقيق في الجرائم الإرهابية ومحاكمتها والبت فيها. وقد وُضعت مبادئ توجيهية وتوصيات لتيسير جمع هذه الأدلة واستخدامها ومشاركتها. ومن هذه المبادئ التوجيهية، على سبيل المثال لا الحصر، المبادئ التوجيهية لتيسير الاستخدام والمقبولية كدليل في المحاكم الجنائية الوطنية للمعلومات التي يجمعها الجيش ويعالجها ويحفظها ويشاركها لمقاضاة الجرائم الإرهابية ("المبادئ التوجيهية للأدلة العسكرية")[18]، التي وضعتها المديرية التنفيذية للجنة مكافحة الإرهاب التابعة للأمم المتحدة والمنتدى العالمي لمكافحة الإرهاب؛ توصيات أبوجا بشأن جمع الأدلة واستخدامها ومشاركتها لأغراض الملاحقة الجنائية للإرهابيين المشتبه بهم ("توصيات أبوجا")[19].

إن المعلومات والأدلة الموجودة في الأجهزة الرقمية متقلبة ويمكن تغييرها بسهولة أو إتلافها أو تدميرها، كما أنها حساسة للوقت، وغير مرتبطة بالمنطقة القضائية. يمكن التلاعب بالمعلومات الرقمية أو حذفها بسهولة دون أي أثر.

تشكل بيئة ميدان المعركة تحديات إضافية عندما يتعلق الأمر بجمع الأجهزة الرقمية والتعامل معها والحفاظ عليها وضمان إمكانية استخدام المعلومات الواردة فيها ومقبوليتها كأدلة في المحاكم، خاصة عندما لا تتوفر خبرة علم الأدلة الجنائية الرقمية وتكون هناك مخاطر تتعلق بالسلامة والأمن.

تعتبر الإجراءات التي يتبعها المستجيبون الأوائل بخصوص جمع الأجهزة الرقمية الموجودة في ميدان المعركة ومعالجتها ذات أهمية خاصة، وتحدد في كثير من الحالات مقبولية المعلومات الموجودة في الجهاز كدليل في الإجراءات الجنائية في قضايا مكافحة الإرهاب.

تعترف توصيات أبوجا بهذا التحدي الخاص المتمثل في ضمان أن المعلومات التي يستردها الجيش والجهات الفاعلة الأخرى المعترف بها في حالات (ما بعد) النزاع تستوفي العتبات القانونية المسموح بها كأدلة في الإجراءات الجنائية، وفقاً للنظام القانوني لمختلف الدول. ويجب استيفاء المعايير القانونية الصارمة المنصوص عليها في القوانين الجنائية الوطنية، والتي تشمل مقبولية الأدلة، والحفاظ على سلسلة العهدة والأدلة، واحترام مبادئ المحاكمة العادلة[20].

يقدم هذا الفصل الظروف والتحديات الفريدة المتعلقة بجمع المستجيبين الأوائل الأجهزة الرقمية في ميدان المعركة، واستخدام المعلومات الموجودة في تلك الأجهزة الرقمية كأدلة مقبولة في الإجراءات القانونية المتعلقة بجرائم الإرهاب.

18 المبادئ التوجيهية لتيسير الاستخدام والمقبولية كدليل في المحاكم الجنائية الوطنية للمعلومات التي يجمعها الجيش ويعالجها ويحفظها ويشاركها لمقاضاة الجرائم الإرهابية، والتي وضعتها المديرية التنفيذية للجنة مكافحة الإرهاب ("المبادئ التوجيهية للأدلة العسكرية")، كانون الأول/ديسمبر 2019.

19 المنتدى العالمي لمكافحة الإرهاب، توصيات أبوجا بشأن جمع الأدلة واستخدام ومشاركتها لأغراض الملاحقة الجنائية للإرهابيين المشتبه بهم، أيلول/سبتمبر 2018.

20 المرجع نفسه، ص 17 في خامساً. توصيات بشأن جمع الجيش للأدلة واستخدامها ومشاركتها.

4 – 2 – 1 ميدان المعركة والأجهزة الرقمية

يتطلب ميدان المعركة من الأفراد العمل في بيئات معقدة ودائمة التغير. وغالباً ما تتميز ديناميكيات ميدان المعركة بالإلحاح والارتياب والفوضى ومستويات عالية من المخاطر. وتتميز مكافحة الإرهاب في ميدان المعركة بالحاجة إلى تحديد التهديدات الإرهابية وتحييدها بسرعة مع التقليل من الأضرار الجانبية والحفاظ على سلامة المدنيين والمناطق المحيطة، في ظل الاحترام الكامل لحقوق الإنسان وسيادة القانون. وفي بعض الأحيان، يستلزم ذلك أيضاً جمع الأجهزة الرقمية الموجودة في ميدان المعركة، إذ قد تحتوي على بيانات ومعلومات مهمة أو ذات صلة بالتحقيق والملاحقة القضائية والبت في الجرائم الإرهابية.

4 – 2 – 2 الجهات الفاعلة في ميدان المعركة

لأغراض هذه الوثيقة، يعني ميدان المعركة البيئة التي تجري فيها إجراءات مكافحة الإرهاب والتي قد يكون فيها الأفراد العسكريون أول المستجيبين بسبب المناطق غير الخاضعة لسيطرة الحكومة أو التي تتسم بنقص الإدارة. وغالباً ما يشمل المستجيبون الأوائل أفراداً عسكريين، ولكن يمكن أن يشملوا أيضاً موظفين مدنيين من المنظمات الوطنية والإقليمية والدولية المكلفة بمكافحة الإرهاب. ويمكن أيضاً لموظفي الجمعيات الأهلية الحضور إلى ميدان المعركة.

يبين ميدان المعركة الفرق بين مسرح الجريمة العادي والظروف الخاصة التي يعمل في ظلها المستجيبون الأوائل ويضبطون أنشطتهم بما يتماشى مع تفويضهم الأصلي.

ولأغراض هذا التقرير، المستجيبون الأوائل هم أي موظفين عسكريين أو مدنيين تابعين لمنظمة حكومية وطنية أو إقليمية أو دولية يكونون أول من يصل إلى مسرح الجريمة الإرهابية والذين يسمح تفويضهم بجمع الأجهزة الرقمية. ولا ينطبق هذا المصطلح على موظفي الطوارئ كرجال الإطفاء وعاملي القطاع الصحي.

تعتبر إجراءات المستجيبين الأوائل ودورهم في جمع الأجهزة الرقمية في ميدان المعركة ذات أهمية قصوى لضمان قبول الأجهزة التي يجمعونها كدليل في إجراءات العدالة الجنائية ويجب أن يكونوا على دراية بالعواقب المتعلقة بسوء التعامل مع جمع الأجهزة الرقمية ونقلها من ميدان المعركة وإليه.

4 – 2 – 3 القيمة المعلوماتية: الاستخبارات مقابل الأدلة

أصبحت المعلومات الرقمية مصدراً مهماً للاستخبارات العسكرية وأدلةً لهيئات إنفاذ القانون. ويمكن استخدام المعلومات الرقمية التي تُجمع في ميدان المعركة كمعلومات استخباراتية تسترشد بها جهود مكافحة الإرهاب وكدليل في الإجراءات الجنائية ضد الإرهابيين.

لا يشمل استخدام المعلومات الرقمية لأغراض استخباراتية أو لأغراض عسكرية أخرى نظامَ العدالة الجنائية ولا يقع ضمن نطاق هذا التقرير. تركز هذه الوثيقة على استخدام المعلومات الرقمية كدليل في الإجراءات الجنائية ضد الجرائم الإرهابية والعتبات القانونية التي ينبغي الوفاء بها كمقبولية الأدلة والحفاظ على سلسلة العهدة والأدلة واحترام مبادئ المحاكمة العادلة[21].

4 – 2 – 4 أبرز التحديات

تولّد مكافحة الإرهاب في ميدان المعركة مجموعة من التحديات البارزة للمستجيبين الأوائل. ويعد جمع الأجهزة الرقمية في ميدان المعركة لأغراض إنفاذ القانون والإجراءات القانونية أحد هذه التحديات الجديدة وغير المألوفة.

وفي حال افتقار المستجيبين الأوائل إلى المعرفة والوعي بالمخاطر والممارسات الجيدة لجمع الأجهزة الرقمية، فإن تصرفاتهم أثناء جمع الأجهزة الرقمية والتعامل معها في ميدان المعركة:

- قد تتسبب في ضرر محتمل لسلامتهم وسلامة الآخرين والبيئة المحيطة.
- قد تؤثر على مقبولية المعلومات الموجودة في الأجهزة الرقمية كأدلة في الإجراءات الجنائية ضد الجرائم الإرهابية.

21 المرجع نفسه.

على سبيل المثال، أنظمة الطائرات بدون طيار أجهزةٌ رقمية، قد يكلف المستجيبون الأوائل بجمعها في ميدان المعركة. يمكن للإرهابيين تفخيخ طائرة بدون طيار لاستهداف المستجيبين الأوائل الذين يحاولون فتح الجهاز في ميدان المعركة أو يمكنهم استخدامها لهجوم ثانوي بمجرد وصول المستجيبين الأوائل إلى موقع الانفجار. وفي العام 2016، انفجرت طائرة مسيرة عندما حاول أفراد الجيش التعامل معها بعد أن تحطمت على الأرض، مما أدى إلى مقتل جنديين وإصابة اثنين آخرين.

يجب أن يكون المستجيبون الأوائل على دراية بالمخاطر المحتملة المرتبطة بالأجهزة الرقمية المتروكة في ميدان المعركة كمخاطر الانفجار وقدرات تتبع الخصوم وغيرها من الوسائل التي يمكن أن تعرض سلامتهم للخطر.

يحتاج المستجيبون الأوائل إلى الالتزام بمجموعة من متطلبات علم الأدلة الجنائية الرقمية للحفاظ على سلسلة العهدة وضمان مقبولية المعلومات، وذلك ليصار إلى استخدام المعلومات المستخرجة من الأجهزة الرقمية المجمعة في ميدان المعركة كدليل في الإجراءات الجنائية.

ومن شأن حسن التوثيق لمكان الحادث وللجهاز الرقمي والإجراءات المتخذة لجمع الجهاز والتعامل معه حتى يسلم إلى المحفوظات أو إلى معمل الأدلة الجنائية أن يضمن الحفاظ على سلسلة العهدة وقبول الجهاز الرقمي والمعلومات كدليل في الدعوى القضائية في المحكمة.

غالباً ما يفتقر المستجيبون الأوائل العاملون في ميدان المعركة إلى التدريب والخبرة والموارد اللازمة لتلبية متطلبات التوثيق المناسبة وقد يعبثون بالأجهزة الرقمية ويجعلونها غير مقبولة كأدلة. على سبيل المثال، من شأن تشغيل جهاز رقمي أو إيقاف تشغيله أو الوصول إلى محتواه أن يغير مصدر الأدلة.

4 – 3 المبادئ التوجيهية

تشكل هذه المبادئ التوجيهية جوهر الوثيقة والإرشادات المعدّة بخصوص جمع الأجهزة الرقمية في ميدان المعركة.

الجدول 4 – المبادئ التوجيهية

المبادئ التوجيهية	
عدم التسبب في ضرر	للحفاظ على سلامة الفريق والمناطق المحيطة به والجهاز وأنظمة التحقيق، يجب التصرف بحذر عند الاقتراب من الجهاز الرقمي الموجود في ميدان المعركة أو لمسه أو تغييره أو توصيله بالشبكات أو أنظمة التحقيق.
الموثوقية	ينبغي إثبات أن المعلومات المستردة من الجهاز الرقمي قابلة لإعادة التوليد ليتم قبول الجهاز الرقمي كدليل. ولذلك، فإن الإجراءات المتخذة على جهاز رقمي في الميدان يمكن أن تؤثر على موثوقيته وتغيير التواريخ أو العناصر الأخرى المخزنة على الجهاز. على سبيل المثال، "الرسائل غير المقروءة".
السلامة	لكي تعتبر المعلومات المستردة من جهاز رقمي بمثابة دليل، ينبغي إثبات عدم العبث بالبيانات أو تعديلها بأي طريقة من شأنها أن تغير معناها أو سياقها.
الأصالة	تشير الأصالة إلى ضمان عدم العبث بالأدلة الرقمية أو تغييرها بأي شكل من الأشكال، وأنها هي ما تبدو عليه. ويعد هذا جزءٌ مهمٌ من مقبولية الجهاز والمعلومات المخزنة فيه. يكون تغيير الجهاز ضرورياً في بعض الحالات لجمعه الجهاز الرقمي، ويجب توثيق الإجراءات المتخذة.
المصداقية	تعبر هذه عن مصداقية الأدلة الرقمية في نظر المحكمة أو هيئة المحلفين. الأدلة ذات المصداقية هي تلك التي تدعمها حقائق وأدلة أخرى ويمكن قبولها على أنها صادقة.
احترام سلسلة العهدة	تشير مقبولية الجهاز الرقمي كدليل إلى ما إذا كانت الأدلة المجمعة من جهاز رقمي تلبي المتطلبات القانونية للمقبولية في المحكمة. قد تختلف معايير المقبولية حسب الولاية القضائية، ولكن بشكل عام، يجب أن تكون الأدلة ذات صلة ومادية وتم الحصول عليها بشكل قانوني، ويجب الحفاظ على سلسلة العهدة.

[خامسا]
جمع الأجهزة الرقمية في ميدان المعركة

5 – 1 لمحة عامة

هذا الفصل إرشادات عملية للمستجيبين الأوائل بخصوص جمع الأجهزة الرقمية في ميدان المعركة بطريقة تقلل من تعطيل الأجهزة الرقمية التي قد تحتوي على معلومات قيمة إلى الحد الادنى وتضمن سلامتها، ويشمل ذلك أدلة التجريم المحتملة والتي يمكن للمحكمة أن تجدها مقبولة في الإجراءات القانونية. سيغطي الدليل أربع مراحل رئيسية:

- المرحلة الأولى: الوصول إلى مسرح العمليات
- المرحلة الثانية: الفرز
- المرحلة الثالثة: جمع الأجهزة وتغليفها
- المرحلة الرابعة: النقل

الشكل 5

5 – 2 الوصول إلى مسرح العمليات

5 – 2 – 1 التخطيط والتحضير

من شأن التخطيط المسبق أن يحسن قدرة المستجيبين الأوائل الذين يجمعون الأجهزة الرقمية في ميدان المعركة وكفاءتهم بشكل كبير وأن يحسّن فرز الأجهزة الرقمية في مكان الحادث. ومن شأن الاستعدادات أن تؤدي إلى زيادة إنتاجية المستجيبين الأوائل في جمع الأجهزة الرقمية وتقليل الوقت اللازم قضاؤه في الموقع والتعرض للتهديدات الأمنية.

إذا كان ذلك ممكناً، أثناء التخطيط والإعداد، يحدد المستجيبون الأوائل أولويات الأجهزة الرقمية المهمة التي يجب جمعها أولاً، وكذلك يحددون الدعم الفني المتاح في الموقع وما قد يحتاجون إليه من مزيد من الموظفين الفنيين والمعدات. يرجى الرجوع إلى الملحق الأول للحصول على قائمة بالأجهزة الرقمية ذات الأولوية في الجمع.

5 – 2 – 2 الوصول إلى مكان الحادث

يجب على المستجيبين الأوائل اتخاذ بعض الإجراءات السريعة الضرورية لسلامتهم وسلامة الآخرين عند الوصول إلى مكان الحادث، ويشار إليها أحياناً باسم "استغلال الموقع":

يجب على المستجيبين الأوائل فحص الموقع بحثاً عن المخاطر المحتملة، وكذلك تحديد الأجهزة الرقمية التي ترسل بالزمن الحقيقي.

يوصى بتوثيق مكان الحادث، ما لم يكن هناك خطر وشيك على سلامة المستجيبين الأوائل والأشخاص الآخرين والمناطق المحيطة وأمنهم، وإجراء تقييم سريع لمكان الحادث.

الجدول 5 – ملخص الإجراءات

الإجراء	الغرض منه	درجة الأهمية
مسح الموقع	إجراءات أمنية	يجب
تحديد الأجهزة الرقمية التي ترسل بالزمن الحقيقي	إجراءات أمنية	يجب
التوثيق	التوثيق	ينبغي
تقييم سريع للمشهد	التعامل	ينبغي

5 – 2 – 3 مسح الموقع

الإطار 1 – إرشادات

يجب إتمام هذا الإجراء قبل الدخول إلى الموقع ويكون هذا أول الإجراءات عند الوصول.

ملاحظة: يمكن دمج مسح الموقع مع الإجراء التالي المتمثل في تحديد الأجهزة الرقمية ذات الإرسال الفوري (انظر 5 – 2 – 4 أدناه).

قد تشكل الأجهزة الرقمية التي تركها الإرهابيون في مكان الحادث تهديداً جسدياً للعاملين في مكان الحادث والمناطق المحيطة به. وكانت هناك حالات خطّط فيها الإرهابيون لهجوم مترادف استهدف الفريق الذي يعمل في الموقع ومنصاته وأدواته التكنولوجية.

يمكن تفخيخ الأجهزة الرقمية وتفجيرها من قبل الإرهابيين باستخدام أجهزة استشعار تتعرف على اقتراب الفريق، أو عن طريق الاتصال الجسدي بجهاز رقمي عندما يلمس المستجيبون الأوائل الجهاز أو يرفعونه، أو عن طريق التحكم عن بعد عندما يراقب الإرهابيون المنطقة أو الجهاز. ويمكن أن يكون تحديد موقع أجهزة تخزين البيانات الإلكترونية بسرعة مفيداً لاستغلالها بشكل أفضل.

قائمة مختصرة للأجهزة التي سيتم مسح الموقع بحثاً عنها:

- الكاميرات (العاملة وغير العاملة)
- الطائرات المسيرة (الطيران أو التشغيل أو الإيقاف)
- أجهزة الاستشعار
- معدات الشبكات: أجهزة التوجيه والخوادم وكابلات الشبكة
- أجهزة الكمبيوتر
- الأجهزة اللوحية
- الهواتف المحمولة
- بطاقات الذاكرة
- ذواكر فلاش
- أجهزة التخزين الرقمية

أ - الغرض

- ضمان أمن المستجيبين الأوائل والموظفين الآخرين والأفراد والمناطق المحيطة وسلامتهم.
- معرفة عدد الأجهزة الرقمية التي سيتم جمعها.

ب - الإجراءات

مسح الموقع أو فحصه بصرياً لتحديد موقع الأجهزة الرقمية المرئية دون الدخول فعلياً إلى مكان الحادث.

ج - النتائج

سيتمكن المستجيبون الأوائل بعد الانتهاء من مسح الموقع من تحديد مخاطر السلامة والأمن الناجمة عن الأجهزة الرقمية المتروكة في مكان الحادث وتعقيدها التكنولوجي وإمكانية مراقبة الإرهابيين الموقع عن بعد. سيكون وجود الكاميرات والطائرات بدون طيار وأجهزة الاستشعار وأجهزة الشبكة مؤشراً على احتمال تنشيط الأجهزة الموجودة عن بعد، وينبغي ألا يدخل المستجيبون الأوائل إلى مكان الحادث قبل أن يطهره الموظفون المعنيون.

وكذلك سيعرف المستجيبون الأوائل كمية الأجهزة الرقمية التي سيجمعونها في مكان الحادث وأنواعها.

5 – 2 – 4 تحديد الأجهزة الرقمية التي ترسل بالزمن الحقيقي والأجهزة المفخخة

قد يراقب الارهابيون المواقع في ميدان المعركة عن بعد وقد يتخذون إجراءات ضد المستجيبين الأوائل عن بعد دون علمهم. ويشكل هذا تهديداً لسلامة المستجيبين الأوائل والأشخاص الآخرين والمناطق المحيطة، وللبيانات التي يمكن العثور عليها في الموقع. قد تنبه الأجهزة الرقمية التي ترسل بالزمن الحقيقي التي تكون موصولة ونشطة في ميدان المعركة الإرهابيين بوصول أول المستجيبين إلى مكان الحادث وتسمح لهم بتنفيذ الهجوم.

يمكن أيضاً للإرهابيين التلاعب بالأجهزة الرقمية التي تخزن البيانات عبر الإنترنت عن بعد لتفجير البيانات أو حذفها أو تشفيرها، ومن هذه الأجهزة الهواتف المحمولة والأجهزة اللوحية وأجهزة الكمبيوتر.

ينبغي على الفريق أن يتصل بخبير طائرات مسيرة كجزء من إجراء "التقييم السريع" (انظر 5 – 2 – 6 أدناه) وإجراء بحث القرب الجغرافي لتحديد موقع المتحكم بالطائرة المسيرة مباشرة.

يرجى أخذ العلم أن تقدم التكنولوجيا يحتم إعادة تقييم هذا المؤشر الخاص بوجود المتحكم بالطائرة بالجوار وعدم اعتباره أمراً مفروغاً منه.

يمكن لكاميرات الإرسال تسجيل تصرفات المستجيبين الأوائل واستخدامها ضدهم ليس فقط بشكل مباشر ولكن أيضاً كإجراء للتعرف على الإجراءات التكتيكية للفريق، ويجب تجنبها.

يُنصح بالبحث عن الكاميرات النشطة قبل دخول الفريق إلى مكان الحادث، على الرغم من أن الكاميرات قد تكون مخفية أو مموهة.

لا يؤثر إخفاء عدسات الكاميرا على المواد الرقمية ولكنه قد يؤثر على إجراءات علم الأدلة الجنائية الرقمية الأخرى مثل جمع الحمض النووي. يُقترح إخفاء عدسات الكاميرا باستخدام قفازات مضادة للكهرباء الساكنة، **إذا أمكن**.

إذا أعطى المستجيبون الأوائل الأولوية لجمع عينات الحمض النووي من الموقع والأجهزة **فينبغي** على الفريق استخدام قفازات مضادة للكهرباء الساكنة، وفصل **جهاز الكاميرا** عن مصدر الطاقة لوقف إرساله والاستعداد لجمعه.

عند فصل الكاميرات عن مصدر الطاقة، **ينبغي** على الفريق التأكد من أن ذلك لا يؤثر على مصدر الطاقة الكامل أو الجزئي للموقع ولا يؤثر على مصدر طاقة يغذي مسجل فيديو رقمي أو جهاز تخزين قريب. يمكن فعل ذلك بعد تأكد أن مصدر الطاقة الذي تم فصله متجه مباشرة إلى الكاميرا وبشكل مرئي وفقط إلى الكاميرا، إذا كانت بطاريتها تعمل فيجب إزالتها. هذه المرحلة مخصصة لاعتبارات السلامة، وفي المرحلة التالية من "التقييم السريع" (انظر 5 – 2 – 6 أدناه)، يمكن للفريق التفكير في فصل مصدر الطاقة على نطاق أوسع أو قطع الاتصال بالشبكة.

قد يؤدي استخدام أجهزة التشويش اللاسلكية القصيرة المدى المحمولة باليد[22] إلى إيقاف أجهزة الإرسال التي ترسل التسجيلات إلى مكان بعيد. ويمكن أن يؤدي إيقاف اتصال الأجهزة إلى منع الأجهزة المفخخة التي يتم تشغيلها عن بعد من الانفجار ومنع مراقبة إجراءات المستجيبين الأوائل في الموقع عن بعد.

أ – الغرض

- ضمان أمن المستجيبين الأوائل والموظفين الآخرين والأشخاص والمناطق المحيطة وسلامتهم.
- التعرف على الأجهزة الرقمية المتصلة في مكان الحادث والتي قد تشكل تهديداً لسلامة الموظفين وأمنهم، وإيقاف إرسال الجهاز إن أمكن.
- التعرف على الأجهزة المتصلة التي قد يتلاعب بها الإرهابيون عن بعد ومنعهم من القيام بذلك.

22 الأدلة الجنائية الرقمية في ميدان المعركة والاستخبارات الرقمية وجمع الأدلة في العمليات الخاصة، كريستيان براتشيني وتيمو فايسينن وميشال سادلون وخير الدين باشي وأغوستينو بانيكو وكريس فان دير ميج وماريو هويس إنتفيلد، مركز إكسلنس للدفاع السيبراني التعاوني التابع لحلف شمال الأطلسي، تالين 2016، الصفحة 39.

ب – الإجراءات

1 – **يجب** على المستجيبين الأوائل تحديد الكاميرات العاملة وأنظمة الطيران المسير وتقييم اتصالها. أما العلامات التي تشير إلى أن الجهاز الرقمي متصل فهي كما يلي:

- الجهاز يعمل أو يبدو أنه في وضع الطيران أو يومض.
- يستخدم الجهاز أجهزة اتصال سلكية أو لاسلكية (واي فاي أو شبكة خلوية أو قمر صناعي أو غير ذلك).

2 – **ينبغي** على المستجيبين الأوائل تغطية وجوههم لإخفاء أنفسهم من التصوير الفوتوغرافي النشط أو تسجيل الفيديو بواسطة الأجهزة المتصلة.

3 – **إذا كان ذلك ممكناً**، إيقاف البث والتسجيلات وعزل الموقع رقمياً. يمكن إيقاف الاتصال عن طريق:

- استخدام أجهزة تشويش إرسال الشبكات والإشارات، ويشمل ذلك نظام تحديد المواقع العالمي.
- فصل الموقع بالكامل عن شبكات الكابلات، وإيقاف تشغيل أجهزة التوجيه وأجهزة توليد الشبكة اللاسلكية أو توسيعها.
- فصل الأجهزة عن مصدر الطاقة.

ج – النتائج

بعد الانتهاء من مسح الموقع، سيتمكن المستجيبون الأوائل من تحديد مخاطر السلامة والأمن الناجمة عن الأجهزة الرقمية المتروكة في مكان الحادث، وكذلك تقييم تعقيدها التكنولوجي وإمكانية مراقبة الإرهابيين الموقع عن بعد. ويعد وجود الكاميرات والطائرات المسيرة وأجهزة الاستشعار وأجهزة الشبكة مؤشراً على إمكانية تنشيط الأجهزة الموجودة عن بعد، ويجب ألا يدخل المستجيبون الأوائل إلى مكان الحادث قبل أن يؤمنه الموظفون المعنيون.

5 – 2 – 5 التوثيق

الإطار 2 – إرشادات

ينبغي اتخاذ هذا الإجراء قبل الانتقال إلى المرحلة التالية.

يعد التوثيق عنصراً أساسياً في الحفاظ على سلسلة العهدة. يعد التوثيق مفيداً في هذه المرحلة للأسباب التالية:

- دعم اتخاذ القرار في الموقع، خاصة بخصوص الجهاز الرقمي وما إذا كان قابلاً للاستغلال ويجب جمعه.
- دعم الأجهزة الرقمية في معمل الأدلة الجنائية الرقمية بشكل أفضل. يمكن أن يساعد التوثيق المعمل في فهم الاختلافات التي يجدها خبراء علم الأدلة الجنائية الرقمية في الجهاز الرقمي وتحديد مالك الجهاز الرقمي، وما إلى ذلك.
- توثيق تدخلات المستجيبين الأوائل في مكان الحادث، في حالة الطعن فيها أثناء الإجراءات القانونية.

يمكن للمستجيبين الأوائل استخدام كاميرات الفيديو لتصوير المشهد والأجهزة لأغراض التوثيق. ويمكن أن يوفر تسجيل الفيديو كل أو معظم المعلومات المطلوبة للتوثيق في مرحلة لاحقة. ويمكن للمستجيبين الأوائل رسم المشهد بدلاً من ذلك.

يجب أن تنشأ أي تغييرات يجريها المستجيبون الأوائل في مكان الحادث عن أسباب تتعلق بالسلامة فقط، ويمكن أن يدعم تسجيل الفيديو المباشر مصداقية الإجراءات وسلسلة عهدة الأجهزة الرقمية.

إذا تعذر تسجيل الفيديو لجميع التغييرات التي أجراها المستجيبون الأوائل، فيستحسن استكمال التسجيل بتقرير مكتوب. إذا لم يكن تسجيل الفيديو متاحاً، فيمكن للفريق التوثيق كتابياً، باستخدام النموذج المتوفر في الملحق ب – 1.

أ – الغرض

- الحفاظ على سلسلة العهدة ودعم أنشطة علم الأدلة الجنائية الرقمية المستقبلية.

ب – الإجراءات

1 – **ينبغي** على المستجيبين الأوائل توثيق المناطق المحيطة بالموقع والأجهزة الرقمية الموجودة كتابياً أو عن طريق تسجيل الفيديو.

2 – **ينبغي** أن يشمل التوثيق في هذه المرحلة ما يلي:

- وصفاً عاماً للموقع.
- موقع الجهاز.
- وصف الجهاز وحالته – يعمل أو في حالة الطيران أو يومض.
- الاتصال الذي تم تحديده في الجهاز – وجود عمليات إرسال عن طريق الشبكة – إشارة إلى الاتصال عن طريق الكابل أو عن طريق أجهزة الاتصال اللاسلكية (واي فاي أو الخلوي أو القمر الصناعي أو غير ذلك).
- الإجراءات المتخذة لعزل الجهاز الذي يرسل عبر الإنترنت والمشهد – توثيق استخدام أجهزة التشويش وقطع التيار الكهربائي، وما إلى ذلك.
- المعلومات التي ظهرت على شاشة الجهاز.
- قائمة مسجلة بأسماء جميع الشهود الموجودين في مكان الحادث عند وصول الفريق – الاسم والكنية وأي إشارة للاشتباه – حالة ذهنية واضحة.

3 – يرجى الرجوع إلى "نموذج التوثيق عند الوصول إلى مكان الحادث" في الملحق ب – 1.

ج – النتائج

توثيق المشهد أو تصويره بالفيديو، ووصف الموقع ومكان الحادث وحالة الأجهزة ووضع اتصال الجهاز وإجراءات المستجيبين الأوائل لفصل الأجهزة وأي شهود حاضرين في مكان الحادث.

5 – 2 – 6 التقييم السريع لمكان الحادث

الإطار 3 – إرشادات

ينبغي اتخاذ هذا الإجراء قبل الانتقال إلى المرحلة التالية للامتثال الكامل لمنهجيات علم الأدلة الجنائية الرقمية. وتجوز بعض الاستثناءات عندما يعرّض البقاء لفترة أطول في مكان الحادث المستجيبين الأوائل أو الأفراد الآخرين للخطر.

هذه هي آخر مراحل الوصول وتبدأ المرحلة التالية وهي فرز الأجهزة الرقمية.

يقتصر الأمر على فصل الكاميرات وأنظمة الطيران المسير عن مصدر الطاقة أو الشبكة، إذ تشكل أكبر خطر للمراقبة عن بعد.

قد تضيع بعض المعلومات عند فصل جهاز رقمي عن مصدر الطاقة أو الشبكة، ولكن هذا ليس الاعتبار الأساسي للكاميرات وأنظمة الطيران المسير.

إن عزل الموقع ضروري لسلامة المستجيبين الأوائل. ويكون العزل الرقمي عن طريق فصل الأجهزة الرقمية عن مصدر الطاقة والشبكة.

إذا كانت هناك كاميرات متصلة بالإنترنت أو طائرات مسيرة في مكان الحادث، فيستحسن التواصل مع خبير الأدلة الجنائية الرقمية في الموقع.

يجب على المستجيبين الأوائل وضع علامة على جميع أنظمة الطيران المسير التي يجمعونها. عادةً ما لا تخزن الكاميرات الثابتة الكثير من البيانات، والكاميرا نفسها أقل أهمية من كمبيوتر تخزين البيانات.

تعتبر الكاميرات عنصراً ذو أولوية منخفضة للجمع.

إذا كان مكان الحادث مراقب أو مفخخ بتقييم المستجيبين الأوائل، فيجب أن يكون قرارهم بمغادرة مكان الحادث أو دخوله وفقاً لبروتوكولات السلامة والأمن المعمول بها.

أ - الغرض

- عزل مكان الحادث عن المراقبة المرئية عن بعد.

ب - الإجراءات

1 - **ينبغي** على المستجيبين الأوائل أن يقرروا أي الأجهزة الرقمية سيفصلون عن مصدر الطاقة أو الشبكة.

2 - **ينبغي** على المستجيبين الأوائل أن يقرروا ما إذا كان هناك حاجة إلى استدعاء خبير في الموقع (كخبير الأدلة الجنائية الرقمية أو أنظمة الطيران المسير أو المتفجرات).

3 - **ينبغي** على المستجيبين الأوائل تحديد الأجهزة الرقمية للفرز.

ج - النتائج

تُفصل الأجهزة الرقمية عن مصدر الطاقة أو الشبكة ويتم تحديدها للفرز. ويستدعى الخبراء المعنيين إلى مكان الحادث، في بيئة آمنة أو مؤاتية.

3 – 5 فرز الأجهزة الرقمية

الفرز عنصرٌ مهم في عملية جمع المستجيبين الأوائل للأجهزة الرقمية. ويستلزم الفرز إجراء تقييم ميداني وتقييم وتحديد أولويات الأجهزة الرقمية أو وسائط التخزين لجمعها ليصار إلى مزيد من الفحص والتحليل. فالفرز يساعد المستجيبين الأوائل على تركيز جهودهم وتوفير الوقت.

ولأغراض هذه الوثيقة، يتضمن الفرز تحديد الأجهزة الرقمية وتحديد أولوياتها في ميدان المعركة لجمعها بناءً على عوامل مثل قيمتها في تحقيقات مكافحة الإرهاب وقيمة البيانات المخزنة.

خلال هذه المرحلة، يجب على المستجيبين الأوائل العثور على جميع الأجهزة الرقمية في الموقع وينبغي عليهم تحديد الأجهزة التي ستجمع ليصار إلى مزيد من الاستغلال والتحليل، وبأي ترتيب للأولوية، ويجب عليهم توثيق إجراءاتهم وكذلك إجراء تقييم سريع لمكان الحادث.

وتجدر الإشارة إلى أن الأجهزة الرقمية لا تحتوي جميعها على بيانات ذات احتمال كبير أن تساعد في الإجراءات الجنائية لمكافحة الإرهاب. قد لا تكون بعض البيانات المخزنة على الأجهزة الرقمية مفيدة، لذلك يجب إعطاء الأولوية لجمع الأجهزة الرقمية وفقاً لجميع الظروف وأولويات الفريق.

في سياق هذه الوثيقة، لا يشمل الفرز العمليات المباشرة أو وصول المستجيبين الأوائل غير المحترفين إلى البيانات الموجودة على الجهاز[23].

23 لمزيد من التفاصيل عن الفرز الميداني مع إمكانية الوصول في الموقع إلى بيانات الجهاز، راجع: الإنتربول، المبادئ التوجيهية للمستجيبين الأوائل في مجال الأدلة الجنائية الرقمية، أفضل الممارسات للبحث عن الأدلة الإلكترونية والرقمية ومصادرتها، آذار/مارس 2021. لمزيد من المعلومات عن تطور الفرز الرقمي، انظر بي كارير. (2011). الفرز في علم الأدلة الجنائية الرقمية: دليل ميداني للمستجيبين الأوائل. سينجرس.

الجدول 6 – ملخص الإجراءات

الإجراء	الغرض	درجة الأهمية
إيجاد جميع الأجهزة الرقمية في الموقع	التعامل	يجب
تحديد الأجهزة الرقمية التي ستجمع	التوثيق	ينبغي
التوثيق	التوثيق	ينبغي
التقييم السريع لمكان الحادث	إجراءات أمنية	ينبغي

5 – 3 – 1 تحديد موقع الأجهزة الرقمية في الميدان

ينبغي على المستجيبين الأوائل البحث عن جميع الأجهزة الرقمية الموجودة في الموقع، ويشمل ذلك الأجهزة المموهة والمخبأة. وفيما يلي قائمة مختصرة لأهم الأجهزة الرقمية ذات الصلة، والتي تخزن الكثير من البيانات وتحتوي على ملفات، والتي يمكن استخدامها كدليل في الإجراءات الجنائية للجرائم الإرهابية:

- الهواتف المحمولة
- أجهزة الكمبيوتر: الثابتة والمحمولة
- الخوادم
- الأجهزة اللوحية
- ذواكر فلاش
- أجهزة التخزين الرقمية
- بطاقات الذاكرة
- بطاقات SIM
- الكاميرات
- الطائرات المسيرة

عندما يجد المستجيبون الأوائل كاميرا ثابتة في الموقع، **يجب** عليهم البحث والعثور على الكمبيوتر (NVR/DVR) الذي ترسل الكاميرات المعلومات إليه. يخزن هذا الكمبيوتر جميع البيانات التي كانت الكاميرات تسجلها حتى توقفها ويجب أن تكون قريبة، وفي بعض الحالات متصلة بكابل بجهاز إنترنت، ويمكن أن يساعد تتبع الكابلات في العثور على جميع الأجهزة الرقمية المتصلة بالإنترنت عن طريق الكابل. عادةً ما تخزن هذه الأنواع من أجهزة الكمبيوتر البيانات المسجلة لفترة وجيزة وتعيد الكتابة على التسجيلات السابقة. هناك طريقة أخرى تتمثل في البحث عن كمبيوتر تخزين الكاميرا عن طريق تتبع كابلات الطاقة للعثور على المزيد من الأجهزة الرقمية المتصلة بمصدر طاقة.

يؤدي تحديد حالة الجهاز الرقمي إلى تحديد الإجراءات المطلوبة لجمع الجهاز.

يجب على الفريق في هذه المرحلة التحقق من حالة الجهاز فقط. ويتم التوثيق خلال المرحلة التالية (انظر 5 – 3 – 3 أدناه).

يعتبر تحديد الأجهزة التي يجب جمعها وأولويتها العنصر الأساسي للفرز. **ينبغي** على المستجيبين الأوائل الامتناع عن إجراء عمليات تفتيش داخل الأجهزة إذا لم يكن في الفريق خبير متخصص في الأدلة الجنائية الرقمية. لتحديد الأجهزة التي سيتم جمعها وبأي ترتيب للأولوية، يجب على المستجيبين الأوائل تقييم الفائدة المحتملة للبيانات المخزنة في الجهاز الرقمي لتحقيقات مكافحة الإرهاب وحالة الجهاز الرقمي.

الجدول 7 – ملخص الاعتبارات

المؤشر	عوامل يجب أخذها بالحسبان	مدى الأهمية	مدى الإلحاح
صلة محتملة للبيانات المخزنة في جهاز رقمي بتحقيقات مكافحة الإرهاب	يشتبه في تورط مالك الجهاز أو مستخدمه في أنشطة إرهابية	أهمية عالية لمزيد من الفحص واستغلال البيانات	–
	تحتوي البيانات الموجودة على الأجهزة الرقمية على ملفات ونشاط المستخدم وبيانات المستخدم والاتصالات	أهمية عالية لمزيد من الفحص واستغلال البيانات	–
حالة الجهاز الرقمي	تالف ومحمي بكلمة مرور ومشفر	أكثر تعقيداً لاستغلال البيانات	–
	مغلق وغير متضرر	أسهل للجمع	غير عاجل
	قيد التشغيل ومحمي بكلمة مرور ويشتبه في أنه مشفر	اتصل بخبير الأدلة الجنائية الرقمية	عاجل جداً

تساعد درجة الأهمية الإجمالية للجهاز الرقمي الفريق في تحديد الأجهزة الرقمية التي يجب التعامل معها أولاً في مرحلة لاحقة، أو التي يجب عدم لمسها على الإطلاق.

في حال الشك بوجود عبوات ناسفة أو أجهزة مفخخة في الموقع، **فيجب** على المستجيبين الأوائل الالتزام بإجراءات السلامة وبروتوكولاتها ذات الصلة.

أ – الغرض

- تحديد موقع جميع الأجهزة الرقمية المتروكة في الموقع وتحديد أولويات جمعها.

ب – الإجراءات

1 – **يجب** على المستجيبين الأوائل البحث في مكان الحادث وتحديد موقع جميع الأجهزة الرقمية.

2 – إذا عثر المستجيبون الأوائل على كاميرا ثابتة في الموقع، **فيجب** عليهم البحث عن الكمبيوتر (NVR/DVR) الذي ترسل الكاميرات المعلومات إليه والعثور عليه.

3 – **يجب** على المستجيبين الأوائل تحديد حالة الأجهزة الرقمية الموجودة في الموقع:

- يعمل
- مغلق
- متصل/غير متصل بشبكة
- متصل/غير متصل بمصدر طاقة
- تالف
- مشفر
- محمي بكلمة مرور

4 – **يجب** على المستجيبين الأوائل تقييم مدى أهمية الجهاز للتحقيق والملاحقة القضائية والبت في الجرائم الإرهابية.

ج – النتائج

1 – تحديد موقع كافة الأجهزة الرقمية في مكان الحادث.

2 – تحديد حالة الأجهزة ورسم أولوياتها من حيث أهميتها في التحقيق والملاحقة القضائية والبت في الجرائم الإرهابية.

5 – 3 – 2 تحديد الأجهزة الرقمية التي ستجمع

يجب على المستجيبين الأوائل دائماً جمع الهواتف الخلوية/المحمولة وأنظمة الطيران المسير ووحدة التحكم عن بعد وأجهزة الكمبيوتر المحمولة وأجهزة الكمبيوتر الثابتة التي تم إيقاف تشغيلها ومستوعبات التخزين مثل ذواكر USB فلاش وبطاقات الذاكرة ومحركات الأقراص الثابتة، لأنها عادةً ما تكون خفيفة الوزن وقد تحتوي على الكثير من المواد الرقمية ذات الأهمية في التحقيق والملاحقة القضائية للجرائم الإرهابية. عادةً ما لا تكون الأجهزة الطرفية كلوحات المفاتيح والفأرة والطابعات وشاشات الكمبيوتر ذات أهمية للاستغلال الرقمي والأدلة الرقمية.

الإطار 4 – إرشادات

قد تكون الأجهزة الرقمية المتروكة في ميدان المعركة ذات قيمة تحقيقية أخرى إلى جانب المعلومات الرقمية. وقد تحمل هذه الأجهزة معلومات الحمض النووي أو بصمات الأصابع أو بقايا المواد المتفجرة، والتي يمكن أن تكون ذات صلة بالتحقيق في الجرائم الإرهابية ومحاكمتها ويجب أخذها في الاعتبار عند اتخاذ قرار بشأن الأجهزة الرقمية التي ستجمع.

في حال العثور على خوادم أو أجهزة كمبيوتر ثابتة قيد التشغيل في الموقع، **فينبغي** على المستجيبين الأوائل استشارة (عن بعد) خبير الأدلة الجنائية الرقمية قبل جمعها. في هذه المرحلة من الفرز، يجب أن تكون الاستشارة كافية، ويمكن أن توفر الأساس لاستدعاء خبير الأدلة الجنائية الرقمية في الموقع لجمع المعلومات. ويتطلب تحديد مدى أهمية الخوادم فرز المعلومات المخزنة، حيث قد يؤدي مثل هذا الإجراء إلى الإضرار بالقيمة الاستدلالية للمعلومات التي ستستخلص منها. وينبغي أن يستند قرار الفرز إلى مدى أهمية الجهاز الرقمي في التحقيق في الجرائم الإرهابية ومحاكمتها، وعلى قدرة المستجيبين الأوائل على تأمين مكان الحادث وانتظار وصول خبير الأدلة الجنائية الرقمية.

قد يؤثر إيقاف تشغيل جهاز الكمبيوتر أو الخادم على القدرة على استعادة البيانات المخزنة عليهما **وينبغي** تجنب ذلك، إذا أمكن لخبير الأدلة الجنائية الرقمية الوصول إلى مكان الحادث.

إذا لم يكن هناك خبير في الأدلة الجنائية الرقمية للتشاور معه، **فينبغي** على المستجيبين الأوائل فصل الجهاز الرقمي عن الشبكة ولكن يجب عليهم إبقائه في حالة عمل إلى أن يتلقوا بعض النصائح من خبير الأدلة الجنائية الرقمية. إذا توجب على المستجيبين الأوائل مغادرة مكان الحادث بشكل عاجل أو إذا لم يكن البقاء في الموقع خياراً جيداً بسبب مخاوف تتعلق بالسلامة والأمن، فينبغي على المستجيبين الأوائل إيقاف تشغيل أجهزة الكمبيوتر العاملة أو إيقاف تشغيلها وجمعها على أي حال. يعد ترك أجهزة الكمبيوتر والخوادم العاملة في الموقع أقل الخيارات ملاءمة.

يجب على المستجيبين الأوائل البحث عن الأجهزة الرقمية التالفة والنظر في مدى أهمية جمعها، **إذا كان ذلك ممكناً**. والأجهزة الرقمية التالفة هي الأجهزة التي تبدو مكسورة أو محترقة أو غير سليمة وما إلى ذلك.

على المستجيبين الأوائل معرفة ما إذا كانت وحدة تخزين البيانات في الجهاز الرقمي التالف تبدو سليمة. إذا كان الجهاز الرقمي في حالة سيئة بشكل واضح، على سبيل المثال، تحطم إلى أجزاء، أو احترق بالكامل، فلن يتمكن المستجيبون الأوائل من تحديد ما إذا كانت البيانات الموجودة على هذا الجهاز لا تزال سليمة. عندما تتعطل الأجهزة الرقمية بالكامل، فإن إعادة بناء الجهاز ليست ممكنة عملياً، **وينبغي** ترك الجهاز في الموقع.

ينبغي على المستجيبين الأوائل النظر في مدى أهمية بيانات الأجهزة الرقمية لمهمات الفريق لتحديد أولويات الأجهزة الرقمية التي يمكن جمعها، وكذلك أهميتها لتحقيقات مكافحة الإرهاب والملاحقة القضائية، إلى جانب إمكانية إعادة بناء الجهاز الرقمي في حال كان تالفاً أو مكسوراً ووزنه المادي والتغليف المطلوب وإجراءات نقله الخاصة.

أثناء الفرز، **ينبغي** على المستجيبين الأوائل وضع علامة على الأجهزة الرقمية التي تقرر جمعها والأخرى التي ستترك في الموقع. سيساعد وضع العلامات على الأجهزة الرقمية أثناء الفرز في التمييز بين العناصر المختلفة الموجودة في الموقع وقد يساعد في توثيق المشهد والمكان الذي تم العثور فيه على الجهاز الرقمي أصلاً والمناطق المحيطة به.

الإطار 5 – إرشادات

قد تبدو العبوات الناسفة في بعض الأحيان وكأنها أجهزة مهملة أو تالفة. **ينبغي** على المستجيبين الأوائل اتباع كافة الاحتياطات الأمنية لتحديد موقع المتفجرات في الموقع واتباع البروتوكولات الأمنية الخاصة بالمواقع التي تنطوي على خطر الانفجار.

أ – الغرض

- تحديد الأجهزة الرقمية التي ستجمع وبأي ترتيب أو أولوية.

ب – الإجراءات

1 – **ينبغي** على المستجيبين الأوائل دائماً تحديد ما يلي ليتم جمعه:
   - الهواتف المحمولة
   - نظام الطيران المسير وجهاز التحكم عن بعد
   - أجهزة الكمبيوتر المحمول
   - أجهزة الكمبيوتر الثابتة التي تم إيقاف تشغيلها
   - مستوعبات التخزين كذواكر USB فلاش وبطاقات الذاكرة ومحركات الأقراص الثابتة
   - بطاقات SIM

2 – **إذا كان ذلك ممكناً**، ينبغي على المستجيبين الأوائل تحديد ما يلي لجمعه:
   - الخوادم
   - أجهزة الكمبيوتر الثابتة التي تم إيقاف تشغيلها

3 – **إذا كان ذلك ممكناً**، ينبغي على المستجيبين الأوائل تقييم الجهاز التالف.

4 – **ينبغي** على المستجيبين الأوائل وضع علامات على الأجهزة التي ستجمع.

ج – النتائج

تحديد الأجهزة الرقمية القابلة للجمع أو تصنيفها للجمع.

5 – 3 – 3 التوثيق

يساعد توثيق الفرز على فهم عملية اتخاذ القرار في الموقع في مرحلة لاحقة ويساعد في تتبع المكونات المفقودة عند استغلال الجهاز الرقمي في المعمل الجنائي. **وينبغي** على المستجيبين الأوائل توثيق عملية الفرز إذا كان ذلك لا يضر بسلامة الفريق وأمنه. إذا كان خبير الأدلة الجنائية الرقمية من بين المستجيبين الأوائل وأجرى الفرز الميداني، **فيجب** توثيق جميع الإجراءات وفقاً لمنهجيات علم الأدلة الجنائية الرقمية.

ستكون هذه الوثائق هامة إذا تم الطعن في الأجهزة الرقمية المجمعة من مكان الحادث في المحكمة أو كانت هناك حاجة لمراجعة قضائية لاحقة. ويمكن أيضاً توثيق الفرز في مرحلة لاحقة. **وينبغي** على المستجيبين الأوائل تسمية جميع الأجهزة الرقمية المخطط جمعها باستخدام ملصقات بسيطة. يمكن استخدام أي نوع من الملصقات الصغيرة البسيطة التي يمكن رؤيتها، ويتعرف الفريق على معناها.

أ – الغرض

- لتوثيق مكان الحادث وجميع الأجهزة الرقمية الموجودة في الموقع وتسمية الأجهزة الرقمية ليصار إلى جمعها.

ب - الإجراءات

1 - **ينبغي** على المستجيبين الأوائل توثيق مكان الحادث من خلال تصويره وجميع الأجهزة الرقمية التي يعثرون عليها، وكذلك الأجهزة التي لن يجمعوها.

2 - **ينبغي** على المستجيبين الأوائل وضع ملصقات على الأجهزة التي سيجمعونها.

ج - النتائج

توثيق كافة الأجهزة الرقمية الموجودة في الموقع وتصنيفها ليصار إلى جمعها.

5 - 3 - 4 إجراء تقييم سريع لمكان الحادث

الإطار 6 - إرشادات

ينبغي اتخاذ هذا الإجراء قبل الانتقال إلى المرحلة التالية للامتثال الكامل لمنهجيات علم الأدلة الجنائية الرقمية. تجوز بعض الاستثناءات عندما يعرض البقاء لفترة أطول في مكان الحادث المستجيبين الأوائل أو غيرهم للخطر.

ينبغي على المستجيبين الأوائل تقييم الحاجة إلى الاتصال بخبراء آخرين قبل البدء في جمع الأجهزة الرقمية. يجب اتخاذ هذه القرارات وفقاً للوقت الذي يمكن للفريق أن يبقى فيه في مكان الحادث، وإذا سمحت الظروف بذلك.

وفي حال العثور على جهاز كمبيوتر أو خادم يعمل، فمن المحتمل أن يؤثر إيقاف تشغيل الجهاز على قدرة فريق الأدلة الجنائية الرقمية على استعادة البيانات المخزنة على هذا الجهاز. لذلك، **ينبغي** على المستجيبين الأوائل استدعاء خبير في الأدلة الجنائية الرقمية في الموقع لجمع المعلومات من أجهزة الكمبيوتر أو الخوادم العاملة لضمان اتباع إجراءات علم الأدلة الجنائية الرقمية بدقة والحفاظ على سلسلة العهدة.

ومن شأن جمع المعلومات من جهاز كمبيوتر أو البحث في الهاتف الخليوي دون التدريب والمعدات المناسبة أن يضر بالبيانات والجهاز، وسيؤثر على موثوقية الأدلة وسلامتها وصحتها، ويجعلها غير مقبولة في الإجراءات الجنائية، ولا ينبغي على المستجيبين الأوائل الذين لم يتلقوا تدريباً على علم الأدلة الجنائية الرقمية القيام بذلك.

في حال العثور على جهاز كمبيوتر أو خادم يعمل، فيجب على المستجيبين الأوائل، **إذا كان ذلك ممكناً**، الاتصال بخبير في الأدلة الجنائية الرقمية للوصول إلى الموقع لإجراء الفرز الميداني للأدلة الجنائية الرقمية ونسخ المعلومات. وإذا اشتبه المستجيبون الأوائل في أن بعض الأجهزة الرقمية قد تكون مفخخة، فيجب عليهم الاتصال بخبراء أو وحدات التخلص من الذخائر المتفجرة.

يعرف المستجيبون الأوائل في نهاية عملية الفرز الأجهزة الرقمية التي ستجمع ويمكنهم تقييم ما إذا كان لديهم موارد كافية لتغليف جميع الأجهزة الرقمية القابلة للجمع ونقلها. وفي حال افتقار المستجيبين الأوائل إلى الموارد، فسيحتاجون إلى طلب المزيد من الموارد ليتم تسليمها في الموقع أو تعديل الفرز وفقاً لذلك. **وينبغي** أن يكون المستجيبون الأوائل على دراية بالتهديدات الناجمة عن العبوات الناسفة أو الأجهزة الرقمية المفخخة. ويجب دائماً اتباع بروتوكولات السلامة والأمن ذات الصلة.

أ - الغرض

- طلب خبرة إضافية قبل جمع الأجهزة الرقمية وتقييم القدرة المادية للفريق لجمع كافة الأجهزة الرقمية القابلة للجمع.

ب - الإجراءات

1 - **ينبغي** على المستجيبين الأوائل أن يقرروا ما إذا كانت هناك حاجة للتشاور مع خبير الأدلة الجنائية الرقمية أو الولوج إلى الموقع.

2 - **ينبغي** على المستجيبين الأوائل أن يقرروا ما إذا كان يجب استشارة خبراء آخرين أو الاتصال بهم في الموقع.

3 - **ينبغي** على المستجيبين الأوائل تقييم قدرتهم البدنية على جمع الأجهزة الرقمية في الموقع من خلال تقييم ما إذا كان لديهم معدات تغليف وقدرات نقل كافية.

ج - النتائج

1 - تم استدعاء خبراء الأدلة الجنائية الرقمية أو غيرهم من الخبراء في الموقع حسب الحاجة قبل جمع الأجهزة الرقمية.

2 - يمتلك المستجيبون الأوائل موارد كافية لتغليف الأجهزة القابلة للجمع ونقلها.

5 - 4 جمع الأجهزة الرقمية وتغليفها

يكون لدى المستجيبين الأوائل وقت أقل بكثير لجمع الأجهزة الرقمية في ميدان المعركة. لذلك ينبغي على المستجيبين الأوائل دائماً جمع أجهزة الكمبيوتر والأجهزة الرقمية في الحالة التي يتم العثور عليها بها وعدم فتحها أبداً في الموقع.

ينبغي جمع الأجهزة الرقمية بحذر منعاً للتلوث والمحافظة عليها. على سبيل المثال، من شأن استخدام المستجيبين الأوائل القفازات المضادة للكهرباء الساكنة أن يزيد من فرص استعادة بصمات الأصابع من الأجهزة الرقمية باستخدام وسائل الأدلة الجنائية التقليدية.

الجدول 8 - ملخص الإجراءات

الإجراء	الغرض	درجة الأهمية
التعامل	التعامل	يجب
توثيق مكان الحادث	التوثيق	يجب
التغليف	التعامل	يجب

5 – 4 – 1 التعامل

الإطار 7 – إرشادات

يجب اتخاذ هذا الإجراء قبل الانتقال إلى المراحل التالية.

"عزل الجهاز رقمياً" إجراءٌ يهدف إلى منع الجهاز الرقمي من إرسال الإشارات واستقبالها.

يجب على المستجيبين الأوائل فصل جميع الأجهزة الرقمية عن الشبكة. ويمكن ذلك عن طريق سحب الكابل أو تغيير حالة الجهاز إلى "وضع الطيران" أو عن طريق تعطيل اتصال الشبكة فيه. ستعمل كل هذه الإجراءات على عزل الجهاز الرقمي عن المناطق المحيطة البعيدة.

بعد قطع الاتصال بالشبكة، **يجب** على المستجيبين الأوائل الاستمرار في اعتبار أن الجهاز الرقمي يستمر في إرسال الإشارات. فحتى في وضع الطيران، يستمر الجهاز الخلوي في إرسال إشارات GPS وقد يشير إلى الموقع الدقيق للمستجيبين الأوائل أو إلى معمل الأدلة الجنائية الرقمية الذي يسلم المستجيبون الأوائل الجهاز إليه.

لضمان اعتراض الإشارات، **يجب** على المستجيبين الأوائل تغليف جميع الأجهزة الرقمية القابلة للجمع في حقيبة فاراداي في أقرب وقت ممكن بعد فصلها عن الشبكة (لمزيد من المعلومات، راجع التغليف 5 – 4 – 3 أدناه). لمنع أي خلط بين الأجهزة، وفي بعض الحالات بين أماكن الحوادث المختلفة، ينبغي على المستجيبين الأوائل وضع ملصقات على الأجهزة وتعبئتها في أكياس إفرادية منفصلة.

يجب أن يتضمن وضع العلامات ما يلي:

- إشعار بوجود "الجهاز الرقمي"
- تاريخ الجمع ووقته
- رقم تعريف فريد للجهاز الرقمي
- الاسم الكامل لعضو الفريق الذي جمع الجهاز
- تعريف فريد ودقيق للموقع الذي تم العثور فيه على الجهاز
- علامة تشير إذا كان ينبغي استنساخ هذا الجهاز أو نسخه

عند التعامل مع **الأجهزة العاملة** التي تحتوي على كاميرات، **ينبغي** على المستجيبين الأوائل دائماً تحويل الكاميرا بعيداً عن وجوههم. وهذا سيمنع الإرهابيين من تصوير أول المستجيبين بالوسائل التلقائية التي عادةً ما ترسل الصور إلى مواقع بعيدة أيضاً. ويجب على المستجيبين الأوائل ضمان وضع ملصق صغير على كاميرا الجهاز المحمول بمجرد الاقتراب منه.

إذا كان **الهاتف الخلوي** قيد التشغيل وهو مفتوح، **فينبغي** على المستجيبين الأوائل إلغاء كلمة مرور الجهاز الرقمي ليتمكنوا من الوصول إليه في مرحلة لاحقة.

ينبغي اعتبار جميع طرازات الهواتف المنتجة بعد العام 2013 مشفرة وينبغي التعامل معها وفقاً لذلك في الموقع (انظر القسم 5 – 3 – 4 أعلاه). **إذا كان ذلك ممكناً**، يجب على المستجيبين الأوائل عدم إغلاق الهواتف المحمولة التي يجمعونها وجمعها في حالة العمل التي تم العثور عليها فيها. **وإذا كان ذلك ممكناً**، على المستجيبين الأوائل إبقاء الهواتف المحمولة نشطة باستخدام مصدر طاقة بديل (شاحن محمول خارجي) حتى يصل الجهاز الرقمي إلى معمل الأدلة الجنائية الرقمية ليصار إلى استغلاله بشكل أفضل.

في حال عدم توفر معمل للأدلة الجنائية في مكان قريب، **ينبغي** على المستجيبين الأوائل الاتصال بخبير الأدلة الجنائية الرقمية لاستغلال الجهاز في الموقع (انظر 5 – 3 – 4 أعلاه).

إذا علم المستجيبون الأوائل كلمة مرور جهاز رقمي أو تمكنوا من إلغائها فيمكنهم إيقاف تشغيله. وإذ كان وصول الهاتف الخلوي الذي تم جمعه إلى معمل الأدلة الجنائية متوقعاً بعد أيام من جمعه **فينبغي** على المستجيبين الأوائل تسمية الجهاز عن طريق كتابة كلمة المرور الخاصة به وإغلاقه قبل التغليف إذا كان ذلك ممكناً.

يتطلب اختراق تشفير الهاتف الخليوي موارد معمل الأدلة الجنائية الرقمية المتقدمة. وفي حال عدم توفر مثل هذا المعمل، **ينبغي** على المستجيبين الأوائل محاولة تحديد هوية مستخدم الجهاز والعثور على كلمة مرور الجهاز. ويجب أن تكون هذه الإجراءات متوافقة مع سيادة القانون، وإذا لزم الأمر، يجب أن تكون مصحوبة بمراجعة قضائية أو أمر قضائي.

ينبغي جمع الهواتف المحمولة مع كابلات الشحن الخاصة بها إن وجدت في الموقع.

عند العثور على نظام طيران مسير في مكان الحادث، سواء كان في حالة عمل أو مغلقاً، يمكن للمستجيبين الأوائل الاتصال بخبير أنظمة الطيران المسير للحصول على معلومات سريعة. ومع ذلك، يجب فحص أنظمة الطيران المسير بواسطة خبير الأدلة الجنائية الرقمية، والذي **ينبغي** استدعاؤه إلى الموقع (انظر القسم 5 – 3 – 4 أعلاه)[24].

عند الاشتباه في أن **جهاز تخزين البيانات** مشفر، **ينبغي** على المستجيبين الأوائل البحث عن كلمة المرور في مكان الحادث واستجواب الشهود ذوي الصلة. ويجب تنفيذ جميع الإجراءات وفقاً لسيادة القانون ومبادئ حقوق الإنسان. وفي حال كان الموقف عاجلاً، فيجب أن يخضع أي تقديم غير طوعي لمعلومات كلمة المرور للمراجعة القضائية.

إذا كان الجهاز عبارة عن **كمبيوتر عامل** وفيه ذاكرة بيانات مشفرة، فعلى المستجيبين الأوائل، **إذا أمكن**، تصوير المعلومات المعروضة على الجهاز والاتصال بخبير الأدلة الجنائية الرقمية للتشاور (انظر القسم 5 – 3 – 4 أعلاه). قد لا يمكن الوصول إلى معلومات الجهاز بعد إيقاف تشغيله، لذا يجب على المستجيبين الأوائل استشارة خبراء الأدلة الجنائية الرقمية قبل إيقاف تشغيل الجهاز أو الكمبيوتر أو فصل مصدر الطاقة عنه.

شاشات الكمبيوتر أجهزة كبيرة الحجم ويصعب نقلها ولا تحتوي عادة على معلومات رقمية ذات صلة بالتحقيقات والملاحقات القضائية. إذا كانت شاشة كمبيوتر عادية، **فلا ينبغي** على المستجيبين الأوائل جمعها، بل يمكنهم تركها في الموقع. **وينبغي** على المستجيبين الأوائل التأكد من أن الشاشة ليست جهاز كمبيوتر متكامل.

يجب اعتبار شاشة الكمبيوتر "المتكاملة" بمثابة جهاز كمبيوتر **وينبغي** على المستجيبين الأوائل جمعها إذا كانت في حالة إيقاف التشغيل أو استشارة خبير الأدلة الجنائية الرقمية في حال كانت عاملة.

في حال العثور على شاشات تلفزيون ذكية في الموقع، **ينبغي** على المستجيبين الأوائل استشارة خبير الأدلة الجنائية الرقمية لتحديد ما إذا كان ينبغي أخذ الشاشة الذكية أم لا.

لا تخزن **الطابعات** عادةً أي معلومات إضافية. وتخزَّن معظم البيانات الموجودة على المستندات المطبوعة على جهاز الإرسال **وينبغي** على المستجيبين الأوائل جمع الأجهزة الرقمية الأخرى كأجهزة الكمبيوتر أو الهواتف المحمولة **وينبغي** أن تكون مجموعة الطابعات ذات أولوية منخفضة. لكن في بعض الأحيان تخزن الطابعات بيانات آخر المستندات المطبوعة. يمكن أن يكون المستند المخزن على الطابعة جزئياً، دون وقت وتاريخ محددين أو دون إشارة إلى المستخدم الذي أرسل المستند للطباعة. **ينبغي** على المستجيبين الأوائل جمع الطابعات فقط في حال عدم توفر أجهزة رقمية أخرى.

على المستجيبين الأوائل التأكد من عدم توصيل الجهاز الرقمي بمصدر طاقة أو مادة متفجرة قبل لمسه أو رفعه.

أ – الغرض

- ضمان سلامة الأجهزة الرقمية التي تم جمعها ومصداقيتها، والحفاظ على سلسلة عهدة المعلومات أو الجهاز وضمان مقبوليتها كدليل في المحكمة.

ب – الإجراءات

1 – **يجب** على المستجيبين الأوائل عزل الجهاز رقمياً.

2 – **يجب** على المستجيبين الأوائل وضع علامات على جميع الأجهزة الرقمية.

3 – **يجب** على المستجيبين الأوائل جمع الأجهزة الرقمية بحذر لتجنب التلوث والمحافظة عليها.

24 انظر أيضاً الإنتربول، المبادئ التوجيهية للمستجيبين الأوائل في الأدلة الجنائية الرقمية، أفضل الممارسات للبحث عن الأدلة الإلكترونية والرقمية ومصادرتها، آذار/مارس 2021، الصفحتين 41–42.

ج - النتائج

جمع الأجهزة الرقمية من مكان الحادث لتغليفها ونقلها إلى معمل الأدلة الجنائية أو موقع مخصص.

5 - 4 - 2 التوثيق

الإطار 8 - إرشادات

يجب اتخاذ هذا الإجراء قبل الانتقال إلى المراحل التالية.

تعد اللمسة الأولى للجهاز الرقمي المرحلة الأكثر أهمية في إجراءات الأدلة الجنائية الرقمية. ويعد توثيق هذه المرحلة أمراً بالغ الأهمية لسلامة الجهاز ومصداقيته ولسلسلة عهدة الأدلة. **ويجب** ضمان قبوله كدليل في الإجراءات الجنائية.

يجب أن يشتمل كل جهاز رقمي يُجمع على المعلومات التوثيقية التالية المرفقة به طوال مراحل سلسلة العهدة، ويشمل ذلك مرحلة التخزين في معمل الأدلة الجنائية، وعندما يفحصه خبراء الأدلة الجنائية الرقمية.

يمكن رفد التوثيق الإلزامي بالملصقات المجهزة مسبقاً وتسجيلات الفيديو والملاحظات في الموقع وتقارير النماذج وقوائم المراجعة والمزيد.

كما هو موضح في الجدول 9 أدناه، يمكن استكمال بعض الوثائق في مرحلة لاحقة وليس في الموقع، ما دام استرجاعها ممكناً قبل تسليم المستجيب الأول الجهاز الرقمي إلى فريق آخر. **وينبغي** على المستجيبين الأوائل توثيق المواصفات التالية:

الجدول 9 - ملخص الإجراءات

المعلومات الموثقة	الإجراءات المقترحة
تاريخ الجمع ووقته: يجب أن يكون هذا دقيقاً قدر الإمكان.	نموذج منظم لكتابة التاريخ والوقت. يمكن ملؤه في مرحلة لاحقة.
الاسم الكامل ورقم التعريف لعضو الفريق الذي تعامل مع الجهاز الرقمي في الفرز والجمع والتغليف والنقل.	يمكن تزويد كل عضو في الفريق بملصقات تعريفية يمكن استخدامها لوضع العلامات والتوثيق في جميع المراحل وتوثيقها في مرحلة لاحقة.
المكان: المنطقة والموقع ومكان الجهاز الرقمي في الموقع والأجهزة أو الكابلات المتصلة.	يمكن تصوير الجهاز قبل جمعه ويمكن إدراج التفاصيل في مرحلة لاحقة.
الوصف: نوع الجهاز الرقمي والشركة المصنعة أو الطراز واللون ورقم الملصق وغير ذلك.	يمكن تصوير الجهاز قبل الجمع أو أثناءه ويمكن إدخال التفاصيل في مرحلة لاحقة باستخدام تقنية التعرف الضوئي على الحروف أو إرفاق الصورة بالنموذج أو من خلال ملء التفاصيل.
حالة الجهاز الرقمي: عامل/مغلق، الإرسال نعم/لا، مقفل/مفتوح، الحالة المادية.	يساعد وجود استمارة منظمة المستجيبين الأوائل في وضع علامة على الوصف من قائمة معدة مسبقاً.
الإجراءات المتخذة في الموقع: التغييرات التي أجراها المستجيبون الأوائل على الجهاز الرقمي كإلغاء كلمة المرور وإيقاف التشغيل والتوصيل بشاحن محمول وقطع الاتصال بالشبكة.	حقول نصية لوصف جميع التغييرات التي أجريت على الجهاز الذي تم جمعه، وذلك للحفاظ على سلسلة عهدته. قد تؤدي الإجراءات الموضحة إلى تغيير الجهاز وقد تؤثر على أصالته أو قد يكون لها عواقب أخرى غير مقصودة. وينبغي ملء هذه الحقول في أسرع وقت ممكن.
التفاصيل: المالك المعروف والوقت والتاريخ الموجود على الجهاز والمواد المشتبه بها التي يجب البحث عنها.	يمكن ملء هذه التفاصيل في مرحلة لاحقة وستساعد في إجراء المزيد من التحقيقات واستغلال المواد بشكل أكبر.

أ - الغرض

- ضمان سلامة الأجهزة الرقمية التي تم جمعها وموثوقيتها ومصداقيتها، والحفاظ على سلسلة عهدة الأدلة وضمان قبولها كدليل.

ب - الإجراءات

- **يجب** على المستجيبين الأوائل توثيق جميع الإجراءات المنفذة على الجهاز للجمع.

ج - النتائج

توثيق جميع الأجهزة الرقمية المجمعة لضمان قبولها كأدلة.

5 - 4 - 3 التغليف

يجب على المستجيبين الأوائل التأكد من أن كل جهاز رقمي يُجمع يحمل ملصقاً بشكل صحيح وفريد (انظر 5 - 4 - 2 أعلاه) قبل تغليف أي جهاز.

يجب تغليف كل جهاز رقمي بشكل منفصل عن الأجهزة الرقمية الأخرى مع كابلاته أو الإضافات الأخرى التي كانت متصلة به عند العثور عليه.

ينبغي على المستجيبين الأوائل جمع أجهزة الكمبيوتر في المستوعبات التي عثروا عليها فيها، **ولا ينبغي** تفكيكها في الموقع.

ينبغي على المستجيبين الأوائل استخدام أكياس مضادة للكهرباء الساكنة لمنع التفريغ الكهربائي الذي قد يضر الجهاز الرقمي أو المناطق المحيطة به أو حتى يسبب انفجاراً ذاتياً. والأكياس المضادة للكهرباء الساكنة الرخيصة الثمن والخفيفة الوزن ويجب اعتبارها جزءاً من مجموعة أدوات المستجيبين الأوائل. كما يمكن استخدام الأكياس الورقية أو الأظرف التي يمكن إغلاقها بدلاً من الأكياس المضادة للكهرباء الساكنة.

ينبغي أن يدرك المستجيبون الأوائل أن الأجهزة الخلوية تستمر في إرسال إشارات نظام تحديد المواقع العالمي حتى عندما تكون في وضع الطيران وأنها قد ترشد الإرهابي بدقة إلى موقع المستجيبين الأوائل في مكان الحادث وأثناء النقل وإلى موقع معمل الأدلة الجنائية الرقمية. يوصى باستخدام حقائب فاراداي كمواد تغليف لمنع الأجهزة الرقمية من إرسال الإشارات.

على المستجيبين الأوائل ضمان أن حقيبة فاراداي المستخدمة مسبقاً تعمل بشكل صحيح قبل الوصول إلى الموقع. ويمكن للمستجيبين الأوائل استبدالها باستخدام رقائق الألومنيوم لتغليف الجهاز الرقمي (ثلاث طبقات على الأقل) بعد تغليف الجهاز في كيس مضاد للكهرباء الساكنة.

على المستجيبين الأوائل حزم الأجهزة الرقمية التي تم جمعها في وحدة تخزين مبطنة لمنع الاهتزاز والأذى المادي. ويمكن استخدام أي نوع من الحشو على أن يكون الجهاز الرقمي مغلفاً بأكياس مضادة للكهرباء الساكنة.

على المستجيبين الأوائل تعبئة الأجهزة الرقمية في عبواتها الأصلية **إذا كان ذلك ممكناً**[25].

يجب تجميع جميع الأجهزة الرقمية مع الوثائق المقترحة في القسم 5 - 4 - 2.

يجب على المستجيبين الأوائل إغلاق العبوة بشريط لاصق لضمان عدم فقدان المستندات أو الكابلات أو الملحقات المعبأة بالجهاز.

على المستجيبين الأوائل وضع علامة على المغلفات، **ويجب** أن تتضمن العلامات ما يلي:

- ملاحظة "جهاز رقمي"
- ملاحظة بأن "الجهاز في حالة العمل" إن أمكن
- ملاحظة بوجود "خطر انفجار - يحتوي على بطارية" عندما يكون الجهاز مزوداً بشاحن محمول أو يحتوي على بطارية
- تاريخ ووقت الجمع
- رقم التعريف الفريد للجهاز

25 انظر أيضاً: الإنتربول، المبادئ التوجيهية للمستجيبين الأوائل في مجال الأدلة الجنائية الرقمية، أفضل الممارسات للبحث عن الأدلة الإلكترونية والرقمية ومصادرتها، آذار/ مارس 2021، الصفحة 20.

- تعريف فريد ودقيق للموقع الذي عُثر فيه على الجهاز
- مكان فريق المستجيبين الأوائل أو اسمه
- الوجهة النهائية للمغلف

قد يكون استخدام مصدر بديل للطاقة (شاحن محمول) لنقل جهاز رقمي في حالة التشغيل خطيراً ويزيد من خطر انفجار البطارية.

ينبغي أن يكون استخدام الشاحن المحمول ونقل الجهاز في حالة التشغيل معروفاً ومدروساً دائماً من قبل جميع الموظفين الذين يتعاملون مع الجهاز.

يجب عدم تعريض الجهاز الرقمي لدرجات حرارة شديدة في حال نقله وهو في حالة التشغيل، سواء مع شاحن محمول خارجي أو دونها.

قبل اتخاذ قرار بشأن ما إذا كان ينبغي نقل جهاز رقمي باستخدام شاحن محمول خارجي، **يجب** على المستجيبين الأوائل أن يأخذوا في الاعتبار مدة الرحلة المتوقعة إلى معمل الأدلة الجنائية الرقمية ودرجة الحرارة المتوقعة أثناء الرحلة ووقت الوصول المقدر.

أ - الغرض

- تغليف كافة الأجهزة الرقمية المجمعة استعداداً للنقل.

ب - الإجراءات

1 - **يجب** على المستجيبين الأوائل تغليف جميع الأجهزة الرقمية الصغيرة في حقيبة منفصلة مضادة للكهرباء الساكنة.

2 - **يجب** على المستجيبين الأوائل استخدام حقائب فاراداي عند الحاجة.

3 - **يجب** على المستجيبين الأوائل تغليف جميع الأجهزة الرقمية التي لا تحتوي على حافظات واقية (الموجودة داخل الحقيبة المضادة للكهرباء الساكنة) في تغليف مبطن.

4 - **يجب** على المستجيبين الأوائل تعبئة جميع الأجهزة الرقمية المغلفة في صندوق أو مظروف أو حقيبة.

5 - **يجب** على المستجيبين الأوائل تعبئة الأجهزة الرقمية مع نسخة من الوثائق.

6 - **يجب** على المستجيبين الأوائل إغلاق الطرد قبل النقل.

7 - **يجب** على المستجيبين الأوائل وضع علامة على الطرد قبل النقل.

ج - النتائج

تصنيف جميع الأجهزة الرقمية المجمعة بشكل فريد وتغليفها بشكل صحيح.

5 - 5 النقل

يجب نقل الأجهزة الرقمية المجمعة في أسرع وقت ممكن من ميدان المعركة إلى مكان آمن للتخزين ومواصلة استغلال المواد.

يمكن للمستجيبين الأوائل أنفسهم أو فريق آخر نقل الأجهزة الرقمية. ويجب الأخذ في الاعتبار أن نقل جميع الأجهزة الرقمية مباشرة إلى معمل الأدلة الجنائية الرقمية غير ممكن، بل يجب نقل الأجهزة إلى منشأة تخزين ومن ثم إلى معمل الأدلة الجنائية الرقمية في أقرب وقت ممكن لاستغلالها.

يجب على المستجيبين الأوائل إعداد جميع المستندات اللازمة قبل نقل الأجهزة الرقمية للتخزين. **ولا يجوز** ترك الجهاز الرقمي الذي تم جمعه دون مراقبة.

يجب إرفاق الوثائق التي أُعدت خلال المراحل السابقة من هذه الإرشادات بالأجهزة ذات الصلة.

ينبغي نقل الأجهزة الرقمية في عبوات مبطنة ومغلقة وبعيدة عن فريق النقل قدر الإمكان لتقليل احتمالية تصويرهم أو تسجيل أصواتهم بواسطة أجهزة التسجيل النشطة.

الجدول 10 – ملخص الإجراءات

الإجراء	الغرض منه	درجة الأهمية
التوثيق	التوثيق	يجب
الأجهزة الرقمية خلال النقل	إجراءات أمنية	يجب
التسليم	التعامل	يجب

5 – 5 – 1 التوثيق

الإطار 8 – إرشادات

هذا الإجراء **واجب**.

يجب توثيق النقل من حيث توثيق مختلَف أعضاء الفريق الذين لمسوا الجهاز الرقمي، والوجهة المحددة كمعمل الأدلة الجنائية والتخزين وما إلى ذلك.

ينبغي أن تتضمن الوثائق وصفاً موجزاً للجهاز الرقمي وأهداف نقله لمساعدة الطرف المتلقي في التعامل مع الجهاز بسرعة.

يجب أن يكون الجهاز مصحوباً بنسخة من الوثائق التي أعدها المستجيبون الأوائل أثناء عملية الاستلام.

5 – 5 – 2 الأجهزة الرقمية خلال النقل

ينبغي أن يكون فريق النقل على دراية بمخاطر نقل الأجهزة الرقمية. ويجب على فريق النقل عدم فك تغليف الأجهزة الرقمية التي تم جمعها أبداً لأنهم بذلك قد يكشفوا أنفسهم للإرهابيين الذين قد يستمروا في تعقب الأجهزة. ويمكن للأجهزة الرقمية غير المغلفة إرسال الإشارات وكشف موقع النقل وتسجيل المحادثات ونقل البيانات إلى موقع معادي غير معروف. وهذا بدوره يمكن أن يؤدي إلى هجمات استهدافية وكشف طريق النقل وموقع المنشأة.

قد يؤدي نزع تغليف الهواتف المحمولة التي لم يتم إخفاء الكاميرا فيها إلى تصوير وجوه أعضاء الفريق ونقل هذه البيانات إلى السحابة الرقمية.

وينبغي أن يكون فريق النقل أيضاً على دراية بمخاطر الأجهزة الذاتية الانفجار كالبطاريات والشاحن المحمول والهواتف الخلوية وما إلى ذلك، واتخاذ الاحتياطات اللازمة.

ينبغي أن تظل الأجهزة الرقمية مغلفة في جميع الأوقات ولا توضع أبداً في حضن أحد أعضاء الفريق.

ينبغي مراقبة درجة حرارة النقل لمنع ارتفاع درجة حرارة الأجهزة الرقمية. قد ترتفع درجة حرارة الجهاز في بعض الظروف الجوية القاسية أو عند وضعه بالقرب من مصدر حرارة أثناء النقل.

5 – 5 – 3 التسليم

يجب الحفاظ على سلسلة العهدة **ويجب** توثيق تسليم الأجهزة الرقمية المجمعة وإرفاقها بالجهاز.

يجب على فريق التسليم إطلاع فرق النقل على آليات السلامة والنقل والتحقق من إرفاق جميع الوثائق والملصقات بالجهاز قبل تسليمه. يعد ذلك ضرورياً لمنع كسر سلسلة العهدة ومنع فقدان الأجهزة وسوء الفهم والارتباك في المستقبل.

[الملحق أ]
قائمة مراجعة المعدات الأساسية

أ - 1 قائمة المراجعة

فيما يلي قائمة مقترحة بالمعدات الأساسية للمستجيبين الأوائل:

- كاميرا فيديو
- قفازات مضادة للكهرباء الساكنة
- ملصقات للكتابة: ملصقات فريدة للموظفين أو ملصقات قابلة للكتابة، علامات دائمة (لوضع العلامات)
- ملصقات صغيرة لتغطية عدسة الكاميرا
- أجهزة تشويش الإرسال المحمولة، ويشمل ذلك شبكة الواي فاي والخلوية ونظام تحديد المواقع العالمي
- أكياس مضادة للكهرباء الساكنة أو أكياس بسحاب أو مظاريف ورقية قابلة للإغلاق
- معدات الختم
- حقائب فاراداي أو أكياس رقائق الألومنيوم أو أغلفة رقائق الألومنيوم
- تغليف الفقاعات
- عبوات مبطنة
- علب كرتون للتغليف
- نماذج التوثيق:
  - توثيق الوصول
  - توثيق جمع الأجهزة الرقمية

[الملحق ب]
نموذج التوثيق

ب – 1 نموذج – التوثيق عند الوصول إلى مكان الحادث

ينبغي على المستجيبين الأوائل أن يوثقوا كتابياً أو عن طريق تسجيل الفيديو المناطق المحيطة بالموقع والأجهزة الرقمية الموجودة.

يجب ملء التالي لكل موقع جمع:

تاريخ ووقت الوصول:

التاريخ	التوقيت

تفاصيل الموقع

المنطقة	الموقع
وصف عام	

الموظف الموثق:

اسم ورقم تعريف عضو الفريق الذي يملأ النموذج والقائد في الموقع

الاسم الكامل	رقم التعريف	الوصف
الاسم الكامل	رقم التعريف	الوصف

توصيف الجهاز وحالته:

الرقم	توصيف الجهاز وحالته مشغل/ مقفل/ مكسور/ طيران	حالة الاتصال على الجهاز	المكان في الموقع	هل هناك حاجة إلى خبرة في الأدلة الجنائية الرقمية لجمع الجهاز؟
		☐ فعال ☐ غير فعال		☐ نعم ☐ لا
		☐ فعال ☐ غير فعال		☐ نعم ☐ لا
		☐ فعال ☐ غير فعال		☐ نعم ☐ لا
		☐ فعال ☐ غير فعال		☐ نعم ☐ لا
		☐ فعال ☐ غير فعال		☐ نعم ☐ لا
		☐ فعال ☐ غير فعال		☐ نعم ☐ لا

الإجراءات المتخذة في الموقع:

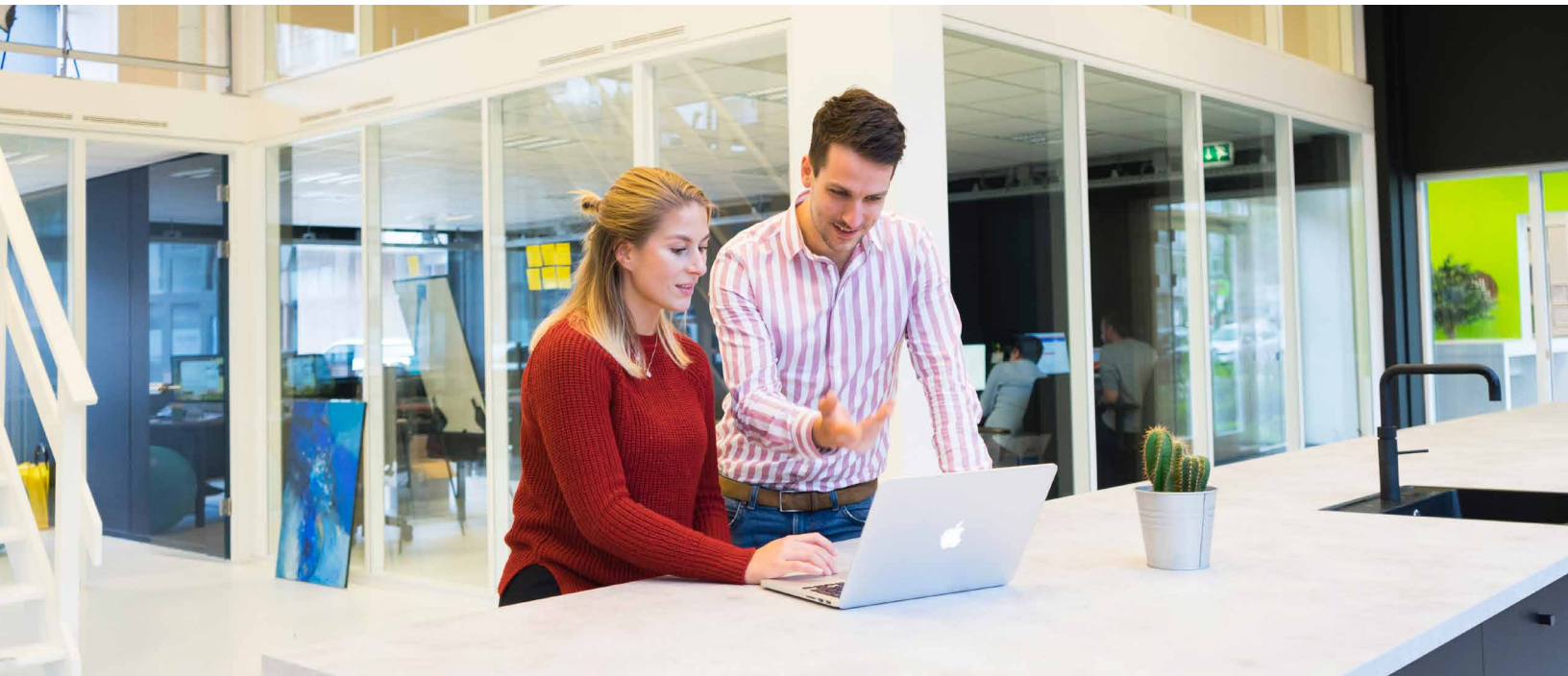
اذكر أي تغييرات أجراها الفريق على الموقع من حيث عزل الشبكة والبث والأجهزة. ويشمل ذلك أي معالجة لجهاز كإلغاء كلمة المرور أو إيقاف تشغيله أو توصيله بشاحن محمول أو فصله عن الشبكة أو غير ذلك.

الشهود:

الاسم الكامل	رقم التعريف	الوصف
الاسم الكامل	رقم التعريف	الوصف
الاسم الكامل	رقم التعريف	الوصف
الاسم الكامل	رقم التعريف	الوصف

الملاحظات

- وصف الجهاز وحالته – معلومات عن الجهاز على الشاشة. يرجى ذكر ما إذا كان الجهاز يعمل أو في حالة الطيران أو يومض، وما إلى ذلك.
- وضع الاتصال على الجهاز – وجود عمليات إرسال الشبكة: إشارة إلى الاتصال عن طريق الكابل أو عن طريق أجهزة الاتصال اللاسلكية (واي فاي أو الشبكة الخلوية أو القمر الصناعي أو غير ذلك).
- الإجراءات المتخذة لفصل إرسال الجهاز عبر الإنترنت في مكان الحادث – توثيق استخدام أجهزة التشويش أو فصل مصدر الطاقة، او غير ذلك.
- قائمة بأسماء جميع الشهود الموجودين في مكان الحادث عند وصول الفريق – الاسم والكنية وأي إشارة للاشتباه – حالة ذهنية ملحوظة.



ب – 2 نموذج – نموذج توثيق جمع الأجهزة الإلكترونية

يجب جمع الأجهزة بحذر منعاً للتلوث وحفاظاً عليها. يهدف هذا النموذج إلى توثيق كل جهاز يُجمع. يمكن إكمال بعض التفاصيل الموجودة في هذا النموذج في مرحلة لاحقة وليس في الموقع، ما دام ذلك يتم قبل تسليم فريق المستجيبين الأوائل الجهاز الرقمي إلى فريق آخر.

أرفق هذا النموذج بعد ملئه مع الجهاز الذي تم جمعه وغلفه مع الجهاز.

ينبغي توثيق كل جهاز رقمي يُجمع

رقم الجهاز كما وجدناه عند الوصول أو الملصق الخاص به

تحقق من أن الرقم مطابق للملصق الموجود على الجهاز

تاريخ الجمع وتوقيته:		
التاريخ	التوقيت	
المسؤول عن التعامل مع الجهاز:		
الاسم الكامل والرقم التعريفي لعضو الفريق الذي تعامل مع الجهاز أو أجرى تغييرات أو اختاره للفرز والتجميع والتعبئة.		
الاسم الكامل	الرقم التعريفي	الوصف
الاسم الكامل	الرقم التعريفي	الوصف
الاسم الكامل	الرقم التعريفي	الوصف
الاسم الكامل	الرقم التعريفي	الوصف
مكان الجمع		
المنطقة	الموقع	
مكان الجهاز في الموقع		
الأجهزة أو الكابلات المتصلة به		
توصيف الجهاز الذي تم جمعه		
نوع الجهاز		
الشركة المصنعة أو الطراز		
اللون	الرقم على اللصاقة	
الحالة	☐ إغلاق	☐ تشغيل
الإرسال	☐ نعم	☐ لا
	☐ مقفل	☐ مفتوح
الحالة المادية		

الإجراءات المتخذة في الموقع:

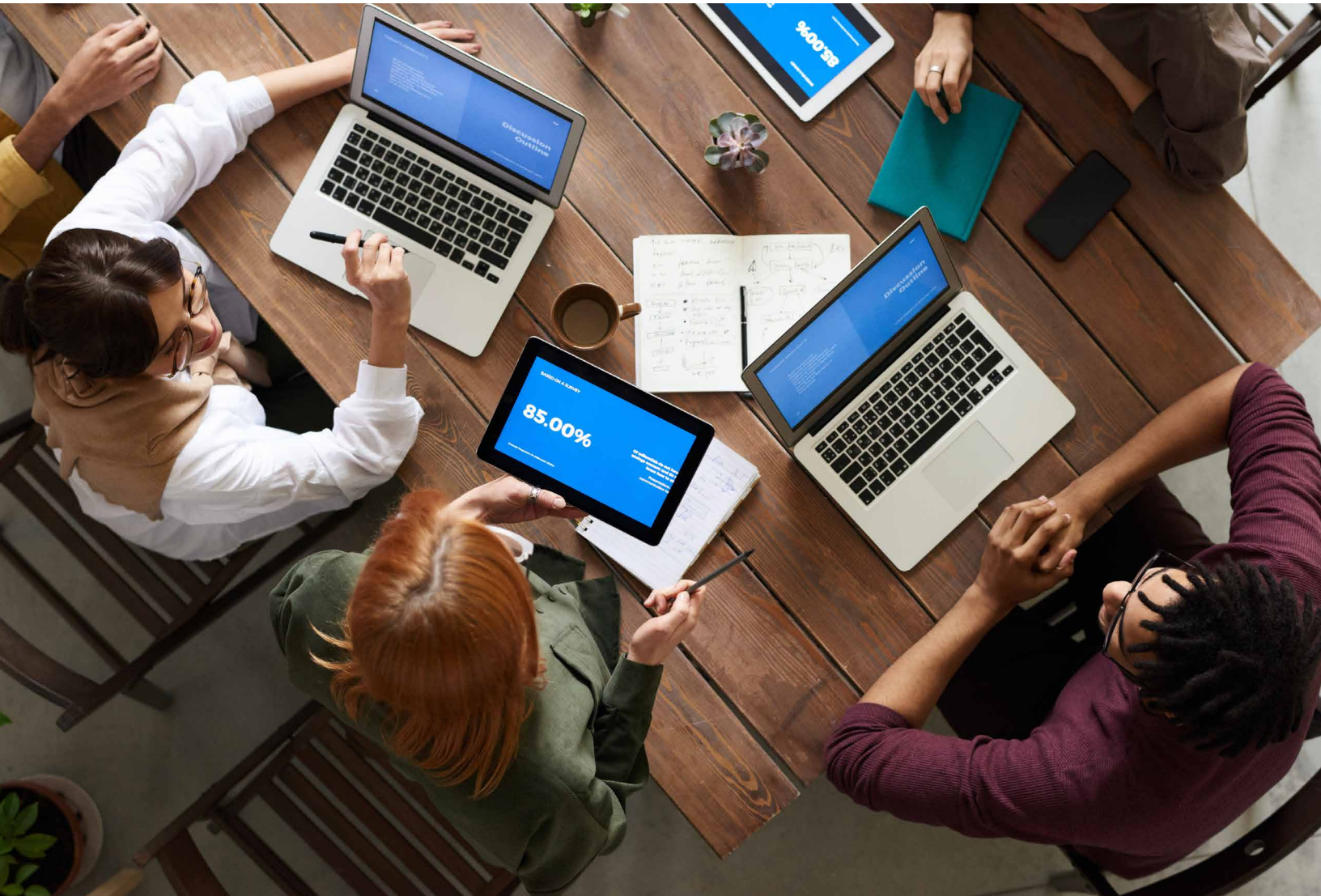
اذكر أي تغييرات أجراها الفريق على الموقع من حيث عزل الشبكة والبث والأجهزة. ويشمل ذلك أي معالجة لجهاز كإلغاء كلمة المرور أو إيقاف تشغيله أو توصيله بشاحن محمول أو فصله عن الشبكة أو غير ذلك.

التفاصيل:

المالك المعروف

الوقت والتاريخ على الجهاز:

ملاحظات:



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

24-11100