أمن المنشآت الحيوية

تأليف
عقيد ركن /فيصل محسن مرجان

الإهداء

بكل فخر واعتزاز أهدي هذا العمل

إلى

المغمورين من رجال المنشآت البواسل الذين يعملون بكل جهد وتفاني، تحت الشمس والظلام، يسهرون لننام، ويضحون لنحيا.

إلى الشهداء الأبرار الذين ارتقوا في ميدان الشرف، وإلى الجرحى الذين حملوا على أجسادهم وسام الفداء، وإلى كل مخلص من رجال الأمن والشرطة والاستخبارات والدفاع المدني.

أنتم السور المنيع، والعين الساهرة، والدرع الذي لا ينكسر.

لكم مني كل التقدير والعرفان

المؤلف

بسم الله الرحمن الرحيم

﴿وَتَعَاوَنُوا عَلَى الْبِرِّ وَالتَّقْوَىٰ

وَلَا تَعَاوَنُوا عَلَى الْإِثْمِ وَالْعُدْوَانِ﴾

سورة المائدة: ٢.

المحتويات:

الوحدة الأولى :مفاهيم أساسية في أمن المنشآت الحيوية

- تعريف المنشآت الحيوية
- أنواع المنشآت الحيوية
- أهمية أمن المنشآت الحيوية
- التهديدات الأمنية المحتملة
- متطلبات تأمين المنشآت الحيوية
- القوانين المنظمة لأمن المنشآت الحيوية
- وضع السياسات والإجراءات الأمنية
- دور أجهزة الدولة ذات العلاقة
- التنسيق مع السلطات المحلية
- الالتزام بالمواصفات والمعايير الدولية

الوحدة الثانية :إجراءات الأمن الوقائي

- تفتيش الأشخاص والمركبات
- تأمين المداخل ونقاط التفتيش
- كاميرات المراقبة وأجهزة الإنذار
- أسوار وبوابات المنشآت
- اجراءات تأمين حرم المنشأة
- أنظمة الإغلاق والتحكم بالدخول
- إضاءة حرم المنشأة ومحيطها
- وسائل الحماية من التهديدات الخارجية
- تأمين مواقع البنية التحتية الحيوية

الوحدة الثالثة :إدارة المخاطر الأمنية

- تحديد المخاطر الأمنية المحتملة
- تقييم مستوى المخاطر الأمنية

- اختبار الخطط والتمارين الأمنية
- آليات الوقاية والسيطرة على المخاطر
- غرفة عمليات إدارة الأزمات
- خطوات التعامل مع حالات الطوارئ
- إجراءات الإخلاء في الحالات الطارئة
- فرق الاستجابة السريعة
- التنسيق مع جهات إدارة الأزمات

الوحدة الرابعة :أمن تقنية المعلومات

- تأمين شبكات وأنظمة المعلومات
- حماية أنظمة التحكم الإلكترونية
- تأمين قواعد البيانات والمعلومات
- خطة استمرارية الأعمال.
- برامج التوعية الأمنية للعاملين
- التدريب على الإجراءات الأمنية
- نشر ثقافة اليقظة والتبليغ
- مشاركة المجتمع المحلي
- التعاون مع وسائل الإعلام

الوحدة الخامسة :الاستخبارات ومكافحة التجسس

- جمع المعلومات الاستخبارية ذات الصلة
- حماية المعلومات والوثائق الحساسة
- مكافحة عمليات تسلل العناصر المعادية
- التنسيق مع أجهزة إنفاذ القانون
- بناء التحالفات الاستراتيجية لتعزيز الأمن

مقدمة الكتاب

تُمثل المنشآت الحيوية شريان الحياة للدول المعاصرة، فهي العمود الفقري الذي تستند إليه استمرارية الخدمات الأساسية للمجتمع، كالطاقة والمياه والغذاء والصحة والاتصالات والنقل، وتشكل الركيزة التي يقوم عليها الأمن القومي والتنمية المستدامة والاستقرار الاقتصادي والاجتماعي. وإزاء ما تشهده الساحة الدولية من تصاعد في حدة التهديدات الأمنية، وتنوع في أساليبها، وتطور في أدواتها، أصبحت حماية هذه المنشآت من الأولويات الاستراتيجية التي لا تقبل التأجيل أو الترف، وأضحت مسؤولية وطنية مشتركة تتطلب تضافر جهود جميع الأطراف، من أجهزة أمنية وحكومية، إلى مشغلين وخبراء، إلى مجتمعات محلية وشركاء دوليين.

وينطلق هذا الكتاب، الذي يقع في خمس وحدات تدريبية مترابطة، من إدراك عميق لحقيقة مفادها أن أمن المنشآت الحيوية لم يعد مجالاً تخصصياً ضيقاً يقتصر على الخبراء الأمنيين، بل صار علماً متشعباً يتقاطع فيه الأمن المادي، والأمن السيبراني، وإدارة المخاطر، والاستخبارات، ومكافحة التجسس، والتوعية المجتمعية، والتخطيط الاستراتيجي، ضمن منظومة متكاملة لا يقوم ركن منها إلا بالآخر. وقد صُمم هذا الكتاب ليكون مرجعاً أكاديمياً متكاملاً، وأداة تدريبية منهجية، للمختصين والعاملين في مجال حماية البنى التحتية الحيوية، وللمسؤولين عن رسم السياسات الأمنية وإدارة الأزمات، وللباحثين والدارسين في العلوم الأمنية والعسكرية والاستراتيجية.

تبدأ الرحلة العلمية للكتاب بالوحدة الأولى تحت عنوان **"مفاهيم أساسية في أمن المنشآت الحيوية "**، حيث يؤسس لفهم شامل لماهية المنشآت الحيوية وأنواعها وأهميتها الاستراتيجية، ويحلل التهديدات الأمنية المحتملة التي تواجهها بمختلف أنواعها ومصادرها، ويستعرض متطلبات تأمينها في ضوء القوانين المنظمة، والسياسات والإجراءات الأمنية، ودور أجهزة الدولة والسلطات المحلية، والالتزام بالمواصفات والمعايير الدولية، مانحاً القارئ خريطة طريق واضحة لفهم مكونات منظومة الأمن الشاملة لهذه المنشآت.

وتنتقل إلى الوحدة الثانية الموسومة بـ **"إجراءات الأمن الوقائي "**، التي تغطي الجانب المادي الملموس في حماية المنشآت، بدءاً من تفتيش الأشخاص والمركبات، وتأمين المداخل ونقاط التفتيش، مروراً بتقنيات المراقبة والإنذار، وأنظمة الإغلاق والتحكم في الدخول، وأسوار وبوابات المنشآت، وإضاءة الحرم، ووسائل الحماية من التهديدات الخارجية، وصولاً إلى تأمين مواقع البنية التحتية الحيوية في مختلف قطاعاتها، لترسم بذلك صورة متكاملة للجدار الدفاعي المادي الذي يشكل خط الدفاع الأول لأي منشأة.

وتأتي الوحدة الثالثة **"إدارة المخاطر الأمنية "**كمنهجية علمية متقدمة تنتقل بالقارئ من مجرد تطبيق إجراءات إلى ممارسة عقلية استباقية، حيث يتم تحديد المخاطر الأمنية المحتملة وتقييمها، ثم اختبار الخطط والتمارين الأمنية، واستعراض آليات الوقاية والسيطرة على المخاطر، وصولاً إلى إدارة الأزمات عبر غرف العمليات المتخصصة، وخطوات التعامل مع حالات الطوارئ، وإجراءات الإخلاء، وتشكيل فرق الاستجابة السريعة، والتنسيق مع جهات إدارة الأزمات، لتجسيد الانتقال من مفهوم الحماية التفاعلية إلى مفهوم المرونة المؤسسية الاستباقية.

وتتجه الوحدة الرابعة نحو الفضاء الرقمي في موضوعها **"أمن تقنية المعلومات "**، فتتناول حماية شبكات وأنظمة المعلومات، وتأمين أنظمة التحكم الإلكترونية(OT) ، وحماية قواعد البيانات والمعلومات، وتطوير خطط استمرارية الأعمال، وبرامج التوعية الأمنية للعاملين، والتدريب على الإجراءات الأمنية، ونشر ثقافة اليقظة والتبليغ، وإشراك المجتمع المحلي، والتعاون مع وسائل الإعلام، إدراكاً بأن التهديدات السيبرانية أصبحت تمثل أخطر تحديات العصر، وأن حماية البنى التحتية الحيوية تتطلب وعياً رقمياً يعادل الوعي المادي إن لم يفقه.

وتُختتم الوحدة الخامسة والأخيرة بعنوان **"الاستخبارات ومكافحة التجسس "**، وهو البعد الاستباقي الاستراتيجي الذي يرفع منسوب الحماية إلى مستوى التوقع والاستباق، إذ تعالج جمع المعلومات الاستخبارية ذات الصلة، وحماية المعلومات والوثائق

الحساسة، ومكافحة عمليات تسلل العناصر المعادية، والتنسيق مع أجهزة إنفاذ القانون، وبناء التحالفات الاستراتيجية لتعزيز الأمن، مانحة القارئ فهماً متقدماً لكيفية مواجهة الخصوم في ميادينهم الخفية، وحماية أسرار المنشأة وكشف مؤامرات الآخرين.

وبين طيات هذه الوحدات الخمس، يسعى هذا الكتاب إلى تقديم رؤية متكاملة لأمن المنشآت الحيوية، تجمع بين العمق النظري والمنهجية العلمية، والتطبيق العملي والواقعي، والتحليل النقدي الموضوعي، معتمداً على أحدث المراجع الأكاديمية والتقارير المهنية، مستشرفاً تطور التهديدات والممارسات الفضلى في هذا المجال الحيوي المتجدد، آملاً أن يكون إضافة نوعية للمكتبة الأمنية العربية، وأداة علمية تسهم في بناء قدرات الكوادر الأمنية، وتعزيز منعة المنشآت الحيوية، ودعم الأمن الوطني في مواجهة التحديات المتعاظمة.

نسأل الله التوفيق والسداد، وأن يكون هذا العمل خالصاً لوجهه الكريم، نافعاً لخدمة الدين والوطن والأمة، إنه ولي ذلك والقادر عليه.

الوحدة الأولى: مفاهيم أساسية في أمن المنشآت الحيوية

تعريف المنشآت الحيوية

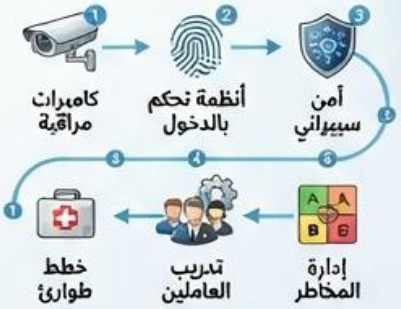
منشآت أساسية لاستمرار الخدمات الحيوية وحماية وحماية الأمن الوطني.

أنواع المنشآت الحيوية

أهمية أمن المنشآت الحيوية

التهديدات الأمنية المحتملة

متطلبات تأمين المنشآت الحيوية



القوانين المنظمة لأمن المنشآت الحيوية

وضع السياسات والإجراءات الأمنية

التنسيق مع السلطات المحلية

دور أجهزة الدولة ذات العلاقة

الالتزام بالمواصفات والمعايير الدولية

الوحدة الأولى: مفاهيم أساسية في أمن المنشآت الحيوية

تمثل المنشآت الحيوية الركيزة الأساسية التي يقوم عليها الأمن القومي للدول، وذلك لما توفره من خدمات وموارد لا غنى عنها للمجتمع، ولما يمكن أن يترتب على تعطيلها أو الإضرار بها من تداعيات كارثية على الصعد الاقتصادية والاجتماعية والبيئية. ويتطلب فهم طبيعة أمن هذه المنشآت إحاطة شاملة بمجموعة من المفاهيم التأسيسية التي تشكل الإطار النظري والتطبيقي لهذا التخصص الدقيق، وهو ما تعمل هذه الوحدة على تقديمه بأسلوب منهجي يراعي الدقة العلمية والأمنية معاً.

أولاً: تعريف المنشآت الحيوية

تعرف المنشآت الحيوية في الأدبيات الأمنية والقانونية بأنها "مجموعة الأصول المادية والتنظيمية والأنظمة التشغيلية التي يتوقف عليها استمرار أداء الوظائف الأساسية للدولة والمجتمع، بحيث يؤدي أي خلل أو تعطل فيها إلى انهيار أو شلل في قطاعات حيوية كالطاقة والمياه والغذاء والصحة والاتصالات والنقل". وتتسم هذه المنشآت بطابع استراتيجي يجعلها هدفاً محتملاً للتهديدات المختلفة، سواء كانت طبيعية أو بشرية المنشأ. وقد توسع مفهومها ليشمل ليس فقط البنى التحتية المادية، بل أيضاً الأنظمة الرقمية وسلاسل الإمداد والموارد البشرية العاملة فيها."1"

ثانياً: أنواع المنشآت الحيوية

يمكن تصنيف المنشآت الحيوية وفق معايير متعددة، منها معيار القطاع، ومعيار الأهمية الاستراتيجية، ومعيار قابلية التعرض للخطر. وعلى المستوى القطاعي، تشمل المنشآت الحيوية قطاعات الطاقة (محطات التوليد، شبكات النقل والتوزيع، منشآت النفط والغاز)، والمياه (محطات التحلية، السدود، شبكات الإمداد)، والغذاء (المزارع الإستراتيجية، مخازن الحبوب، مصانع الأغذية الأساسية)، والصحة (المستشفيات المركزية، مخازن الأدوية، مراكز المختبرات)، والاتصالات وتقنية المعلومات (مراكز البيانات، كابلات الاتصالات البحرية، أقمار الصناعة)، والنقل (المطارات، الموانئ، شبكات السكك الحديدية)، بالإضافة إلى المنشآت الحكومية الحيوية والمراكز المالية والمصرفية. ويستند هذا التصنيف إلى معايير دولية معتمدة

في تحديد البنى التحتية الحرجة، مع إمكانية تعديله وفقاً لخصـــوصـــية كل دولة واحتياجاتها الوطنية."2"

ثالثاً: أهمية أمن المنشآت الحيوية

تتجلى أهمية أمن المنشـــآت الحيوية في كونه يمثل خط الدفاع الأول عن اســـتقرار الدولة واستمراريتها، إذ أن أي إخلال في مستوى الأمن المقدم لهذه المنشآت يمكن أن يؤدي إلى عواقب وخيمة تمتد آثارها إلى كافة شـــرائح المجتمع. ومن الأبعاد الأســاســية لهذه الأهمية نذكر البعد الاقتصــادي، حيث ترتبط هذه المنشــآت بالناتج المحلي الإجمالي والاســـتثمارات الوطنية والأجنبية، والبعد الاجتماعي المتمثل في توفير الخدمات الأساسية للمواطنين، والبعد السياسي المرتبط بثقة المواطنين في مؤسسات الدولة وقدرتها على حماية مقدراتهم، والبعد البيئي حيث يمكن أن تؤدي الحوادث في بعض هذه المنشآت إلى كوارث بيئية، والبعد الأمني القومي الذي يجعل منها عنصــراً أســاســياً في منظومة الدفاع والأمن الوطني. وقد أشــارت العديد من الدراسات إلى أن تكلفة الإهمال الأمني لهذه المنشآت تفوق بكثير تكلفة توفير أنظمة الأمن الوقائي لها."3"

رابعاً: التهديدات الأمنية المحتملة

تتعرض المنشـــآت الحيوية لمجموعة متنوعة ومتطورة من التهديدات، تتفاوت في طبيعتها ومصــادرها ودرجة تأثيرها، ويمكن حصـرها في أربع فئات رئيسـية. الفئة الأولى هي التهديدات الطبيعية، وتشـــمل الزلازل والفيضـــانات والعواصـــف والأعاصـــير وحرائق الغابات، وهي تهديدات لا يمكن منع حدوثها ولكن يمكن التخفيف من آثارها عبر أنظمة الإنذار المبكر والتخطيط للاســـتمرارية. الفئة الثانية هي التهديدات البشـرية غير المتعمدة، والتي تنشـأ عن أخطاء بشـرية أو إهمال أو نقص في التدريب أو سـوء إدارة التشـغيل. أما الفئة الثالثة فتمثل التهديدات البشـرية المتعمدة، وتشـمل الأعمال الإرهابية والتخريبية، والهجمات السـيبرانية، والتجسـس الصـناعي والسـياسـي، وعمليات الاقتحام والتسـلل، وسـرقة المواد أو المعلومات الحساسـة. وتشـير الإحصـاءات الأمنية إلى تصـاعد ملحوظ في الهجمات السـيبرانية

الموجهة للبنى التحتية الحيوية في السنوات الأخيرة. أما الفئة الرابعة فهي التهديدات المزدوجة والتي تجمع بين أسباب طبيعية وأخرى بشرية، كالكوارث التكنولوجية الناجمة عن أعطال في أنظمة التحكم أو انفجارات أو تسربات كيميائية، وهي من أخطر الأنواع لأنها تجمع بين عنصر المفاجأة وصعوبة السيطرة."4"

خامساً: متطلبات تأمين المنشآت الحيوية

يتطلب تأمين المنشآت الحيوية نهجاً شاملاً ومتكاملاً يجمع بين عدة متطلبات رئيسية، تبدأ بمرحلة تقييم المخاطر وتحديد الأصول الحرجة وتصنيف التهديدات المحتملة، وتتلوها مرحلة تصميم الأنظمة الأمنية المادية التي تشمل الأسوار والحواجز ونقاط التفتيش وكاميرات المراقبة وأجهزة الكشف المختلفة وأنظمة التحكم في الدخول. وتأتي بعد ذلك أنظمة الأمن الإلكتروني والتقني، والتي تشمل حماية الشبكات وأنظمة المعلومات، وأنظمة الإنذار المبكر، وأمن نظم التشغيل والتحكم الصناعية، والتشفير وحماية البيانات، فضلاً عن أنظمة الاتصالات الأمنية الطارئة. ولا يمكن إغفال عنصر الأمن البشري والمتمثل في تأهيل القوى العاملة الأمنية، وتدريب العاملين في المنشأة على الإجراءات الأمنية، وزرع الثقافة الأمنية لديهم، وفحص الخلفيات الأمنية للموظفين. كما يتطلب الأمر تطوير خطط الاستجابة للطوارئ، والتي تشمل خطط الإخلاء والتعامل مع الحوادث وإدارة الأزمات، وخطط التعافي واستمرارية العمل بعد الأزمات، فضلاً عن التنسيق مع الجهات المعنية. ويشكل التقييم المستمر والتحسين الدوري جزءاً لا يتجزأ من هذه المتطلبات، لمواكبة تطور التهديدات والتغيرات في طبيعة المنشآت نفسها."5"

سادساً: القوانين المنظمة لأمن المنشآت الحيوية

تتضافر جهود التشريع الوطني مع المعايير الدولية لتشكيل الإطار القانوني والتنظيمي لأمن المنشآت الحيوية. فعلى المستوى الوطني، تسن الدول قوانين خاصة بحماية البنى التحتية الوطنية، وقوانين لمكافحة الإرهاب والجرائم الإلكترونية، وتشريعات تنظيمية تصدرها الهيئات المختصة بكل قطاع، إلى جانب قوانين العمل والسلامة المهنية التي تتضمن أحكاماً أمنية. وتستند هذه القوانين إلى معايير دولية

معتمدة من منظمات كالمنظمة الدولية للمعايير (أيزو)، والمنظمة الدولية للشـــرطة الجنائية (الإنتربول)، ووكالات الأمم المتحدة المعنية. وقد أسـهمت الاتفاقيات الدولية في توحيد الجهود وتبادل الخبرات في هذا المجال، كما أســـهمت تجارب الدول المتقدمة في إثراء القوانين الوطنية، مع مراعاة الخصـوصـية الوطنية في كل دولة. ومن التحديات التي تواجه المشــرعين في هذا الصــدد، مواكبة التطور التكنولوجي المتسارع، وضمان التوازن بين متطلبات الأمن وحماية الحقوق والحريات، وتطوير آليات الرقابة والامتثال الفعالة."6"

سابعاً: وضع السياسات والإجراءات الأمنية

تمثل السـياسـات والإجراءات الأمنية العمود الفقري لنظام أمن المنشـآت الحيوية، إذ تترجم الرؤى الأمنية إلى خطط تنفيذية قابلة للتطبيق. وتبدأ عملية وضـع السـياسـات بتحديد الأهداف الأمنية بوضـوح، ومن ثم بناء هيكل تنظيمي لتطبيق هذه السـياسـات يتضمن تحديد الصلاحيات والمسؤوليات. وتشمل السياسات الأمنية سياسات التحكم في الوصـول، وسـياسـات التعامل مع المعلومات الحسـاسـة، وسـياسـات أمن تقنية المعلومات وسـياسـات اسـتخدام الأجهزة، وسـياسـات الإبلاغ عن الحوادث الأمنية، وســياســات التعامل مع الزوار والمقاولين. وتتحول هذه الســياســات إلى إجراءات تشــغيلية مفصــلة في شــكل تعليمات العمل الأمني ودليل الإجراءات، والتي تغطي سيناريوهات متنوعة لكيفية الاستجابة للتهديدات والحوادث الأمنية بمختلف درجاتها. ومن الخصـــائص الجوهرية للســـياســـات الأمنية الفعالة المرونة اللازمة لتحديثها وتطويرها بشـكل دوري، ووضـوحها بحيث يفهمها جميع المعنيين، وقابليتها للقياس والتقييم، فضلاً عن تطبيقها بعدالة وحياد دون تمييز."7"

ثامناً: دور أجهزة الدولة ذات العلاقة

يتوزع دور أجهزة الدولة في حماية المنشـــآت الحيوية بين جهات متعددة تتكامل أدوارها وتتضـــافر جهودها، حيث تقوم وزارة الداخلية والأجهزة الشـــرطية بدور المحور الأســـاســـي من خلال توفير الحماية الأمنية المباشـــرة، وجمع المعلومات الاســـتخبـاريـة، والتحقيق في الحوادث، وتنفيـذ القوانين الأمنيـة. وتتولى أجهزة

الاستخبارات والأمن الوطني دوراً استباقياً في كشف التهديدات قبل وقوعها وتحليل المخاطر، وتقدير التهديدات الاستراتيجية وتتبع الشبكات الإجرامية والإرهابية. ويأتي دور الجهات المختصة بالأمن السيبراني في حماية الفضاء الإلكتروني للمنشآت الحيوية ومواجهة الهجمات الإلكترونية وتأمين البنى التحتية الرقمية. كما تسهم وزارة الدفاع في حماية المنشآت ذات الأهمية القصوى، خاصة عند ارتفاع منسوب التهديدات الأمنية. وتلعب هيئات الطوارئ والدفاع المدني دوراً حيوياً في التعامل مع الكوارث والحوادث الكبرى وجهود الإخلاء والإنقاذ. ولا يقتصر الدور على الأجهزة الأمنية والعسكرية، بل يشمل الوزارات المعنية كوزارة الطاقة والموارد المائية ووزارة الصحة وهيئة الطيران المدني والهيئات الناظمة للقطاعات المختلفة، حيث تضطلع كل منها بوضع معايير الأمن الخاصة بقطاعها ومتابعة تنفيذها، فضلاً عن هيئة الرقابة ومكافحة الفساد التي تسهم في مراقبة أداء الأجهزة الأمنية وضمان النزاهة في تطبيق السياسات الأمنية."8"

تاسعاً: التنسيق مع السلطات المحلية

يمثل التنسيق مع السلطات المحلية أحد الركائز الأساسية لنجاح منظومة أمن المنشآت الحيوية، وذلك لأن هذه المنشآت تقع غالباً ضمن نطاق ولاية السلطات المحلية. ويأخذ هذا التنسيق عدة أشكال، منها مشاركة السلطات المحلية في لجان الأمن المشتركة، وتبادل المعلومات الاستخبارية والمخاطر المحتملة مع الجهات الأمنية المركزية، وتخطيط وتنفيذ التدريبات المشتركة للاستجابة للطوارئ. وتبرز أهمية هذا التنسيق في أوقات الأزمات، حيث تلعب السلطات المحلية دوراً كبيراً في إدارة الأزمة على المستوى الميداني وتنظيم جهود الإجلاء والإيواء الطارئ للمتضررين، إضافة إلى مسؤوليتها في إعادة تأهيل البنية التحتية للمنشأة المتضررة وتقديم الدعم الخدماتي للمنطقة المحيطة بها. وقد أثبتت التجارب العملية أن نجاح إدارة الأزمات في المنشآت الحيوية يرتبط بشكل كبير بمدى جاهزية السلطات المحلية وقدرتها على التعامل مع الأحداث الطارئة، مما يستلزم إدماجها في منظومة الأمن منذ مراحل التخطيط الأولى وليس فقط وقت حدوث الأزمات."9"

عاشراً: الالتزام بالمواصفات والمعايير الدولية

يشكل الالتزام بالمواصفات والمعايير الدولية رافعة أساسية لتطوير أمن المنشآت الحيوية وضمان تحقيق المستويات المطلوبة من الحماية والأمان، حيث تساعد هذه المعايير على توحيد المفاهيم والممارسات وتقييم الأداء الأمني بموضوعية، كما تسهل تبادل الخبرات والتجارب الناجحة بين الدول المختلفة. ومن أبرز المعايير الدولية في هذا المجال، معايير سلسلة (أيزو ٣١٠٠٠) لإدارة المخاطر، ومعايير سلسلة (أيزو ٢٧٠٠١) لأمن المعلومات، ومعايير (IEC 62443) لأمن نظم التحكم الصناعية، وبروتوكولات المنظمة الدولية للطاقة الذرية وأمن المنشآت النووية. وتستند هذه المعايير إلى مبادئ أساسية كنهج تقييم المخاطر المستند إلى الأدلة، وأخذ الدروس المستفادة من الحوادث السابقة بعين الاعتبار، ومراعاة التطور التكنولوجي المتسارع، وضمان التوازن بين الأمن وكفاءة التشغيل. ويتطلب الالتزام بهذه المعايير إجراء تقييمات دورية من جهات معتمدة، وتطوير خطط طموحة للوصول إلى مستويات متقدمة من الامتثال، مع الأخذ في الاعتبار أن بعض هذه المعايير قد يحتاج إلى تكييف مع الظروف الوطنية دون الإخلال بجوهرها."10"

الوحدة الثانية:

إجراءات الأمن الوقائي

كاميرات المراقبة وأجهزة الإنذار

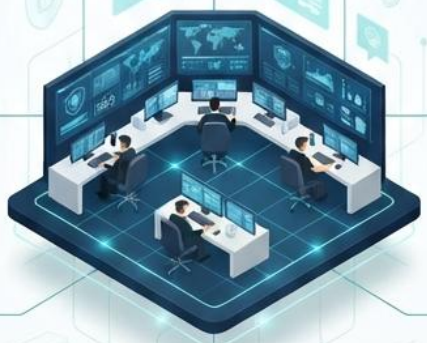
أنظمة CCTV متطورة، حساسات، ولوحات تحكم ذكية.

تأمين المداخل ونقاط التفتيش

بوابات أمنية متقدمة وحواجز إلكترونية وأفراد أمن مدربون.

تفتيش الأشخاص والمركبات

إجراءات فحص دقيق للأفراد والمركبات عند الدخول.



أسوار وبوابات المنشآت

أسوار أمنية محكمة، بوابات إلكترونية، وأسلاك شائكة.

أسوار وبوابات المنشآت

أسوار أمنية محكمة، بوابات دوارة، ولوحات وأحلاك شائكة.

أنظمة الإغلاق والتحكم بالدخول

بوابات أمنية، مناطق محظورة، ولوحات إرشادية ذات الوجه.

أنظمة الإغلاق والتحكم بالدخول

استخدام البطاقات الذكية، البصمة، والتعرف على الوجه.

إضاءة حرم المنشأة ومحيطها

إضاءة أمنية كافية وكشافات LED لضمان الرؤية الليلية.

وسائل الحماية من التهديدات الخارجية

حواجز خرسانية، أنظمة كشف التسلل، ومراقبة ذكية.

تأمين مواقع البنية التحتية

حماية منشآت الطاقة، المياه، الاتصالات، ومراكز البيانات.

الوحدة الثانية: إجراءات الأمن الوقائي

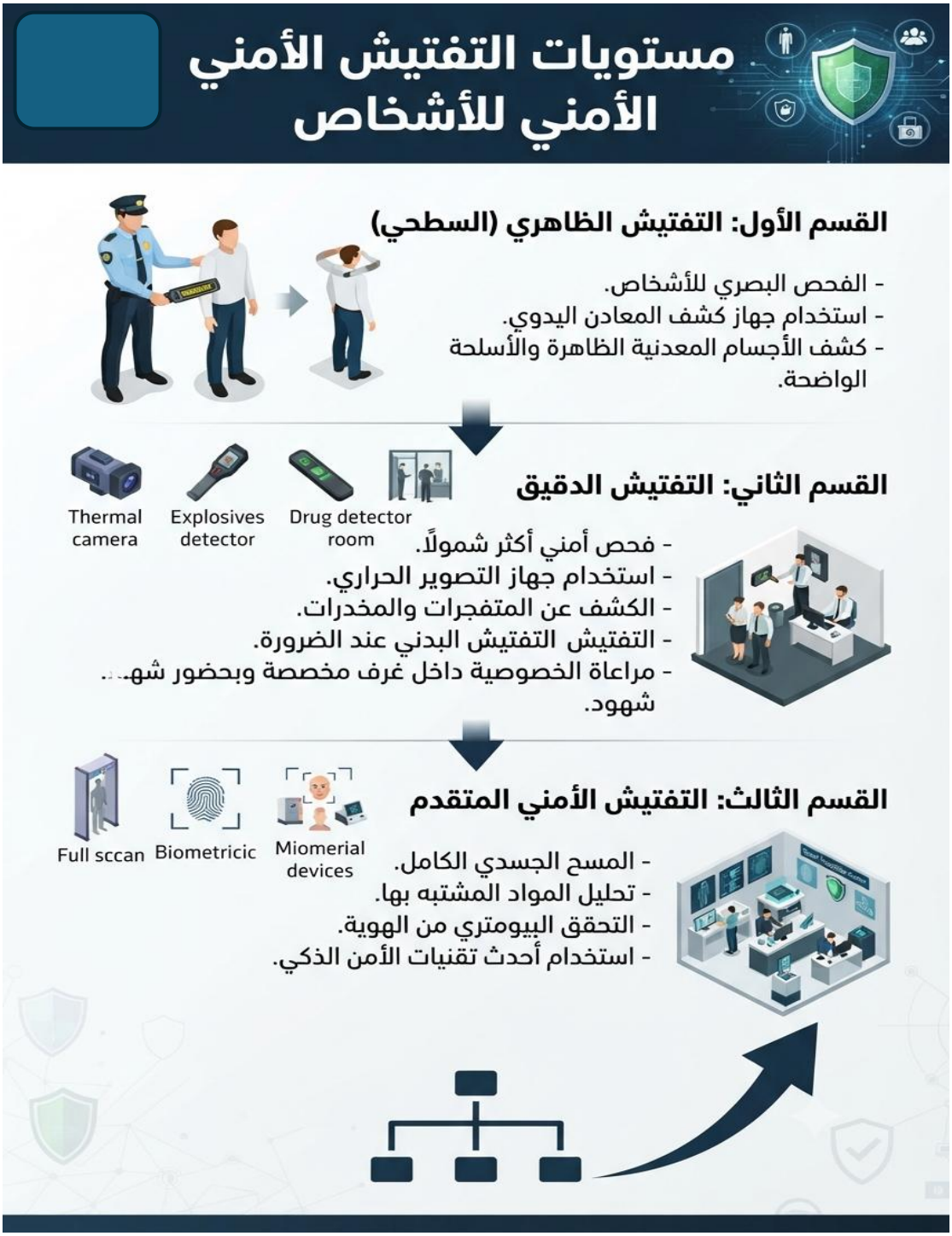
تمثل إجراءات الأمن الوقائي الركيزة الأساسية في منظومة حماية المنشآت الحيوية، إذ تعمل على منع وقوع الحوادث الأمنية قبل حدوثها، وتقليل فرص النفاذ غير المصرح به، واكتشاف التهديدات في مراحلها المبكرة. وتتسم هذه الإجراءات بطابعها الاستباقي الذي يميزها عن الإجراءات العلاجية أو التصحيحية، حيث يتم تصميمها وتطبيقها بناءً على تقييم دقيق للمخاطر ونمذجة للتهديدات المحتملة. وتشمل إجراءات الأمن الوقائي مجموعة مترابطة من العمليات الأمنية التي تغطي كافة نقاط الدخول والخروج، والأشخاص والمركبات والبضائع، والأنظمة الإلكترونية والتقنية، والعناصر البشرية في المنشأة. ويُعد التفتيش أحد أبرز هذه الإجراءات وأكثرها شيوعاً، لما يلعبه من دور محوري في كشف ومنع تسريب المواد غير المرغوب فيها، وتحديد هوية الأفراد والتأكد من صلاحياتهم، ومنع دخول الأدوات أو المواد التي قد تشكل خطراً على سلامة المنشأة."1"

أولاً: تفتيش الأشخاص والمركبات

يشكل تفتيش الأشخاص والمركبات خط الدفاع الأول في تطبيق إجراءات الأمن الوقائي، إذ يُجرى عادةً عند نقاط الدخول الرئيسية للمنشآت الحيوية كالمداخل والمخارج وبوابات الدخول المخصصة. ويتطلب هذا الإجراء تخطيطاً دقيقاً وتنظيماً محكماً يجمع بين السرعة والكفاءة، مع مراعاة الجانب الإنساني وكرامة الأشخاص الخاضعين للتفتيش، لضمان استمرارية تدفق العمل وعدم التسبب في تأخيرات غير مبررة.

وتندرج عملية تفتيش الأشخاص تحت عدة أنواع رئيسية، يختلف تطبيقها وفقاً لمستوى التهديد المقدّر وطبيعة المنشأة وموقعها. فالتفتيش الظاهري أو السطحي يُجرى بصرياً وباستخدام أجهزة الكشف عن المعادن المحمولة باليد، ويكتفي بالكشف عن الأجسام المعدنية الواضحة والأسلحة الظاهرة. أما التفتيش الدقيق فيشمل فحصاً أكثر عمقاً يستخدم أجهزة التصوير الحراري وأجهزة الكشف عن المتفجرات والمخدرات، وقد يتضمن تفتيشاً بدنياً مع الحفاظ على الخصوصية عبر

غرف مخصصة وبحضور شهود. في حين أن التفتيش الأمني المتقدم يستخدم تقنيات المسح الجسدي الكامل وأجهزة تحليل المواد والتحقق البيومتري من الهوية، ويطبق غالباً في المنشآت ذات التصنيف الأمني الأعلى."2"



أما بالنسبة لتفتيش المركبات، فشهد تطوراً ملحوظاً في السنوات الأخيرة بفضل التقدم التكنولوجي، حيث انتقل من التفتيش البصري المعتمد على الخبرة البشرية إلى استخدام أنظمة المسح بالأشعة السينية وأجهزة الكشف عن المتفجرات في المقطورات والشاحنات، وكاميرات المسح الأرضي لكشف التغيرات في هيكل المركبة، وأجهزة قياس الإشعاع والمواد الكيميائية. ويتم تنظيم عملية تفتيش المركبات عبر عدة مراحل: تبدأ بمرحلة التوقف والفحص المبدئي عن بعد، ثم مرحلة إجراء التفتيش باستخدام الأجهزة التقنية، وتنتهي بمرحلة التقييم الأمني واتخاذ القرار بالسماح بالدخول أو الرفض والإحالة للتحقيق. وفي جميع الأحوال، يجب أن يكون التفتيش وفق إجراءات موحدة ومُوثقة، لضمان عدم التمييز وتكافؤ الفرص بين جميع مرتادي المنشأة. كما يُوصى بإجراء تفتيش عشوائي للمركبات الخارجة من المنشأة لمنع تسريب الممتلكات أو المواد الحساسة، مع مراعاة التدرج في الإجراءات وفقاً لمستوى التهديد وإمكانيات المنشأة المادية والبشرية."3"

ثانياً: إجراءات التحقق من الهوية وصلاحيات الدخول

يتكامل تفتيش الأشخاص والمركبات مع إجراءات التحقق من الهوية وصلاحيات الدخول، لتشكيل ما يمكن اعتباره نظاماً أمنياً متكاملاً لإدارة الدخول. ويقوم هذا النظام على ثلاث ركائز أساسية: عنصر المعرفة ككلمات المرور والأرقام السرية، وعنصر الحيازة كالبطاقات الذكية والمفاتيح الإلكترونية، وعنصر القياسات الحيوية كبصمات الأصابع ومسح الشبكية والتعرف على الوجه. وتُستخدم هذه العناصر منفردة أو مجتمعة لتحقيق مستويات متفاوتة من التأمين، إذ يُوصى باستخدام نموذج المصادقة متعددة العوامل للمنشآت الحيوية ذات الحساسية العالية.

وتتم عملية التحقق عبر عدة مراحل منهجية تبدأ بتقديم الفرد لوثيقة هوية رسمية سارية المفعول، تليها مرحلة مطابقة المعلومات مع قواعد البيانات الأمنية والتأكد من عدم وجود بلاغات أو قيود أمنية، ثم مرحلة المصادقة على الصلاحية عبر الأنظمة الإلكترونية، وأخيراً مرحلة التقييم الأمني المتكامل وحسم قرار السماح بالدخول أو المنع. ويزداد التعقيد الأمني مع ضرورة التمييز بين أنواع الدخول

المختلفة كدخول الموظفين الدائمين، ودخول الزوار والمقاولين، ودخول شـــاحنات التموين والنقل، ودخول ســـيارات الطوارئ. ولكل نوع من هذه الأنواع إجراءات تفتيش وتحقق تختلف في درجتها وطبيعتها، مع إمكانية تطبيق نظام المســـتويات الأمنية المتدرجة في منح الصلاحيات، بما يضمن مبدأ "أقل الصلاحيات الضرورية" تحقيقاً للأمن مع الإبقاء على كفاءة التشغيل."4"

ثالثاً: إجراءات أمن المحيط والأسوار والحواجز المادية

تمثل الحواجز المادية والأسوار وأنظمة أمن المحيط العنصر الأكثر ظهوراً وانتشاراً في إجراءات الأمن الوقائي، إذ تشكل خط الدفاع الأول المادي الذي يهدف إلى ردع المتسللين وتأخيرهم ومنع الوصول غير المصرح به إلى مرافق المنشأة الحساسة. وتتنوع المواد والأنظمة المستخدمة في هذا المجال، وتشمل الأسوار الخرسانية أو المعدنية بارتفاعات متفاوتة تتراوح بين ٢,٥ إلى ٥ أمتار حســب مســتوى التهديد، وأنظمة الكشـف الإلكترونية المحيطية المكونة من كاميرات حرارية ومسـتشـعرات اهتزاز وكاشـــفات حركة، والحواجز الميكانيكية كالحواجز الخرســـانية المتحركة والأعمدة القابلة للســـحب لمنع اقتحام المركبات، وأنظمة الإضـــاءة الطارئة التي تضمن استمرارية الرؤية، والمناطق العازلة الآمنة التي تفصل بين المحيط الخارجي والداخلي للمنشأة.

وتعتمد فعالية هذه الإجراءات على مبدأ "الدفاع المتعمق"، حيث تُصـــمم طبقات متعددة من الحماية تبدأ من المحيط الخارجي وصولاً إلى قلب المنشأة، بحيث يتطلب اختراق كل طبقة جهداً ووقتاً متزايدين، مما يمنح أفراد الأمن فرصـــة كافية للاســتجابة. وتخضــع هذه الأنظمة لصــيانة دورية واختبارات مســتمرة لضــمان جاهزيتها في جميع الأوقات، مع الأخذ في الاعتبار الظروف البيئية والمناخية للمنطقة، وطبيعة النشاط داخل المنشأة. كما يُنصح بإجراء مراجعة دورية لتصاميم هذه الحواجز، لتقييم مدى قدرتها على مواجهة التهديدات المستجدة، ولاسيما في ظل تطور أساليب الاختراق واستخدام تقنيات متطورة من قبل الجهات المهددة."5"

رابعاً: إجراءات أمن النظم الإلكترونية والرقابة

مع التحول الرقمي المتسارع في إدارة المنشآت الحيوية، أصبحت إجراءات أمن النظم الإلكترونية جزءاً لا يتجزأ من منظومة الأمن الوقائي. وتشمل هذه الإجراءات حماية شبكات الاتصالات الداخلية، وأنظمة التحكم والإشراف، وقواعد البيانات الحساسة، وأنظمة المراقبة بالفيديو، وأجهزة إنذار الحريق والسرقة. كما تتضمن إجراءات تأمين أنظمة التشغيل والتحكم الصناعية والتي تُعد من أكثر الأهداف تعرضاً للهجمات الإلكترونية، حيث يمكن أن يؤدي اختراقها إلى تعطيل عمليات الإنتاج أو التوزيع أو التسبب في حوادث خطيرة.

وتقوم هذه الإجراءات على عدة مبادئ رئيسية، منها مبدأ التحديث المستمر للبرمجيات وأنظمة الحماية، ومبدأ إدارة صلاحيات الوصول إلى البيانات والأنظمة وفق مبدأ "الحد الأدنى من الصلاحيات"، ومبدأ التشفير القوي للبيانات أثناء التخزين والنقل، ومبدأ المراقبة والرصد المستمر للأنشطة المشبوهة وتحليل السجلات الرقمية، وأخيراً مبدأ وضع خطط للاستجابة للحوادث الإلكترونية للتعامل مع أي اختراق محتمل بأسرع وقت ممكن. وتتضمن منظومة الأمن الإلكتروني أيضاً توعية العاملين وتدريبهم على المخاطر الإلكترونية وأساليب التصدي لها، حيث يُعد العنصر البشري الحلقة الأضعف في سلسلة الأمن الإلكتروني، ولذا تستثمر المنشآت في برامج التوعية الأمنية المستمرة لرفع مستوى الوعي بين العاملين لديها."6"

خامساً: إجراءات التوعية والتدريب الأمني للعاملين

تستكمل إجراءات التوعية والتدريب الأمني للعاملين إجراءات الأمن الوقائي الأخرى، حيث تهدف إلى تعزيز ما يُعرف بالثقافة الأمنية داخل المؤسسة. وتقوم هذه الإجراءات على مبدأ أن الأمن مسؤولية جماعية لا تقتصر على أفراد الأمن فقط، بل تمتد لتشمل كل فرد في المنشأة. وتشمل برامج التوعية تزويد العاملين بمعرفة أساسية بالتهديدات الأمنية التي قد تواجه المنشأة، وتعريفهم بإجراءات الإبلاغ عن الممارسات المشبوهة أو الحوادث الأمنية البسيطة، وتدريبهم على كيفية التصرف في حالات الطوارئ كالإخلاء أو التعامل مع الحريق أو التهديدات الإرهابية.

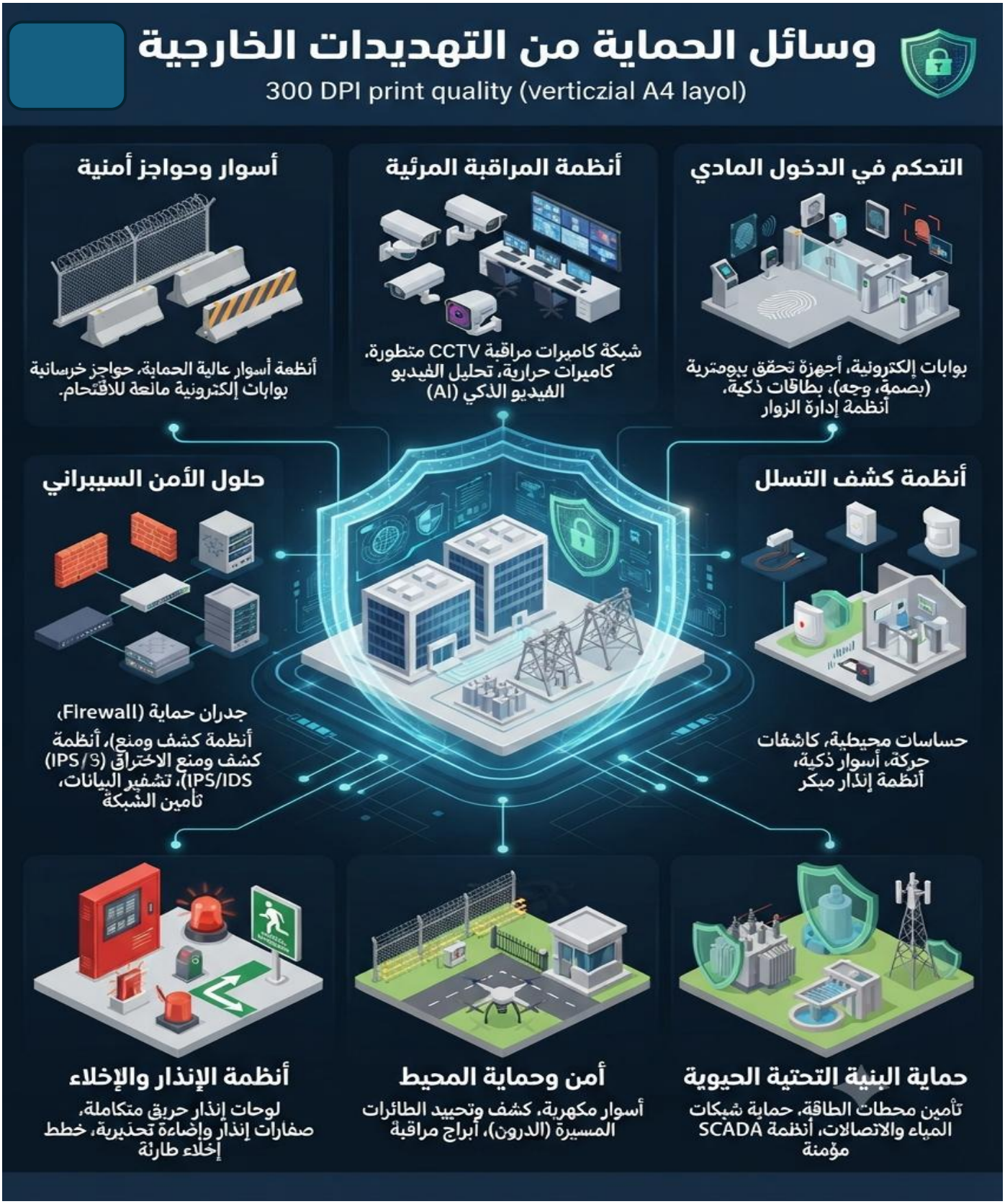
وتأخذ هذه البرامج أشكالاً متعددة كالمحاضرات التوعوية الدورية، والمنشورات والملصقات التذكيرية، والنشرات الإخبارية الأمنية، وورش العمل التطبيقية، والمحاكاة والتدريب العملي على سيناريوهات افتراضية، والاختبارات الدورية لقياس مدى استيعاب الموظفين للمفاهيم الأمنية. ويُعد التدريب العملي المنتظم عنصراً حيوياً في هذا السياق، إذ يمكن العاملين من اكتساب المهارات اللازمة للاستجابة السريعة والفعالة في حالات الطوارئ، كما يعزز ثقتهم بقدراتهم على التصرف تحت الضغط. ويوصى بإجراء هذه التدريبات بشكل دوري ومنتظم، لا سيما للموظفين الجدد أو المنقولين إلى مواقع حساسة، مع توثيق نتائج هذه التدريبات واستخدامها لتطوير السياسات والإجراءات الأمنية بشكل مستمر."7"

سادساً: إجراءات التفتيش الوقائي للبضائع والمهمات

تمثل عمليات تفتيش البضائع والمهمات الواردة إلى المنشآت الحيوية أو الصادرة منها ركيزة وقائية بالغة الأهمية، نظراً لقدرتها على منع إدخال مواد خطرة كالمتفجرات والمواد الكيميائية والأسلحة والمخدرات، وكذلك منع تسريب المعلومات أو الممتلكات الحساسة إلى خارج المنشأة. وتشمل هذه الإجراءات تفتيش الحاويات والشحنات الواردة باستخدام أجهزة الكشف المتطورة والفحص العشوائي بالكلاب المدربة، وتدقيق الفواتير ووثائق الشحن للتأكد من مطابقتها للبضائع الفعلية ومنع التلاعب، وتطبيق إجراءات العزل والفحص المسبق للشحنات الواردة قبل السماح بإدخالها إلى المناطق الداخلية.

وتكتسب إجراءات تفتيش البضائع أهمية خاصة في المنشآت التي تتعامل مع مواد خطرة أو استراتيجية كالمفاعلات النووية ومصانع الأسلحة والمرافق الكيميائية والمخازن الاستراتيجية للغذاء والدواء. ويُوصى بإنشاء مناطق مخصصة لفحص البضائع بعيداً عن المرافق الحيوية، وتزويدها بأجهزة الكشف الحديثة، وتدريب الكوادر العاملة عليها تدريباً متخصصاً. كما ينبغي تطبيق إجراءات أمن سلسلة التوريد ابتداءً من المصدر إلى غاية الوصول، وذلك بالتعاون مع الجهات الموردة

والمشـــغلة للنقل، لضـــمان ســـلامة الشـــحنات طوال رحلتها ومنع أي عبث بها قبل وصولها إلى المنشأة."8"



سابعاً: مراقبة الدخول والخروج وتنظيم الحركة

تكتسب عمليات مراقبة الدخول والخروج وتنظيم الحركة داخل المنشأة أهمية كبرى في إجراءات الأمن الوقائي، حيث تتيح تتبع حركة الأشخاص والمركبات في جميع الأوقات، وتحديد أماكن تواجدهم، والتحقق من التزامهم بالمناطق المصرح لهم بدخولها. وتتم هذه المراقبة عبر نظام متكامل من نقاط التفتيش، وكاميرات المراقبة المنتشرة، وأجهزة تسجيل الدخول والخروج الإلكترونية، إلى جانب الدوريات الأمنية المنتظمة أو العشوائية داخل أروقة المنشأة.

ويستند هذا النظام إلى عدة مبادئ تنظيمية، منها تطبيق نظام المناطق الآمنة متدرجة التصنيف، بحيث تُقسم المنشأة إلى مناطق ذات مستويات حماية مختلفة، ويُسمح لكل فرد بدخول المناطق التي تتناسب مع صلاحياته الأمنية فقط. ويشمل ذلك أيضاً مراقبة حركة الزوار وتقييد تحركاتهم بمرافقين معتمدين، ومنع التصوير أو جمع المعلومات في المناطق الحساسة، وتطبيق نظام تسجيل الدخول والخروج الإلكتروني مع إمكانية التتبع الفوري. ويُعد الربط بين نظام مراقبة الدخول وأنظمة الإنذار وأنظمة الاتصالات أمراً حيوياً لضمان استجابة سريعة ومنسقة عند حدوث أي خرق أمني أو حالة طارئة."9"

ثامناً: إجراءات التأمين على نظم الاتصالات والإنذار المبكر

تُعد أنظمة الاتصالات والإنذار المبكر جزءاً جوهرياً من إجراءات الأمن الوقائي، إذ تتيح كشف الحوادث الأمنية في مهدها والاستجابة لها بأسرع وقت ممكن قبل تفاقمها. وتشمل هذه الأنظمة شبكات الاتصالات الداخلية الآمنة التي تربط جميع نقاط المراقبة والتفتيش بغرفة التحكم المركزية، وأنظمة الإنذار التلقائي للحرائق وكشف الغازات والتسربات، وأنظمة الاتصال الطارئ برجال الأمن والإسعاف والدفاع المدني، وكذلك الربط مع مراكز القيادة والتحكم التابعة للجهات الأمنية العليا. وتستند هذه الأنظمة إلى مبدأ التكرار والتعددية في وسائل الاتصال، بحيث لا يؤدي تعطل إحدى الوسائل إلى شل المنظومة بأكملها، فضلاً عن اعتمادها على مصادر طاقة احتياطية لضمان استمراريتها في حال انقطاع التيار الكهربائي.

وتخضـع هذه الأنظمة لاختبارات دورية منتظمة للتحقق من جاهزيتها وفعاليتها، مع إجراء تحديثات تقنية مسـتمرة لمواكبة التطورات في مجال الاتصـالات وأمن المعلومات. ويلعب مركز التحكم الرئيسـي دوراً محورياً في هذه المنظومة، حيث يقوم بتلقي كافة التنبيهات والإنذارات، وتحليلها واتخاذ القرارات المناسـبة، وتوجيه الفرق الميدانية وتنسـيق تحركاتها، والتواصـل مع الجهات الخارجية عند الحاجة. وتُعقد اجتماعات دورية بين مسؤولي الأمن في المنشأة والجهات المعنية، لتقييم أداء أنظمة الإنذار والاتصـالات، واسـتعراض الدروس المسـتفادة من الحوادث السـابقة سواء وقعت في المنشأة نفسها أو في منشآت مماثلة."10"

تاسعاً: إجراءات التفتيش الدوري والمراجعة الأمنية المستمرة

تضمن عمليات التفتيش الدوري والمراجعة الأمنية استمرارية فعالية إجراءات الأمن الوقائي والتكيف مع التغيرات في مستويات التهديد. وتشمل هذه الإجراءات جولات تفتيشية منتظمة وغير مجدولة على جميع مرافق المنشأة، واختبارات دورية لأنظمة الأمن المادية والإلكترونية، ومراجعة سـجلات الدخول والخروج وكشـف أي مخالفات أو ثغرات، وتحليل الحوادث الأمنية البسـيطة واسـتخلاص الدروس منها، وتقييم أداء الكوادر الأمنية ومدى التزامهم بالإجراءات.

وتُعد المراجعة الأمنية المسـتمرة أداة أسـاسـية لتحسـين الأداء وتطوير السـياسـات، وذلك من خلال تحديد نقاط الضعف المحتملة، وتقييم مدى مناسبة الإجراءات القائمة للتهديدات الحالية والمستجدة، وتحديث خطط الطوارئ في ضـوء المتغيرات، وتقييم فعالية برامج التدريب والتوعية. كما يُنصـح بإجراء مراجعات أمنية شـاملة بشـكل دوري بالاستعانة بجهات استشارية خارجية محايدة، للحصول على تقييم موضوعي لمنظومة الأمن الوقائي وتوصـيات للتطوير، خاصـة بعد وقوع حوادث كبرى في منشـآت مماثلة، أو عند حدوث تغيرات جوهرية في طبيعة المنشـأة أو نشـاطها أو محيطها الجغرافي."11"

عاشراً: إجراءات التنسيق الأمني الداخلي والخارجي

تتوج إجراءات الأمن الوقائي بمنظومة التنسيق الأمني، التي تشمل التنسيق الداخلي بين جميع إدارات وأقسام المنشأة، والتنسيق الخارجي مع الجهات الأمنية والحكومية والخدمية ذات العلاقة. ويضمن هذا التنسيق وحدة الجهود وتكامل الأدوار، وتجنب الازدواجية أو الفجوات في التغطية الأمنية، وتبادل المعلومات الاستخبارية والتحذيرية بشكل فاعل، وتوحيد خطط وإجراءات الطوارئ بين جميع الأطراف المعنية.

وتتخذ آليات التنسيق أشكالاً متعددة، منها عقد اجتماعات تنسيقية دورية ولجان أمنية مشتركة، وربط أنظمة المراقبة والإنذار مع غرف العمليات الخارجية، وإجراء تدريبات مشتركة لمحاكاة سيناريوهات الأزمات، ووضع بروتوكولات موحدة للتعامل مع الحوادث الأمنية. ويتميز التنسيق الفعال بأنه لا يقتصر على أوقات الأزمات، بل يمتد ليشمل مراحل التخطيط والبناء الوقائي، والمشاركة في تقييم المخاطر وتحليل التهديدات، والتطوير المستمر للسياسات والإجراءات الأمنية. كما يُعد التنسيق مع السلطات المحلية والمجتمع المحيط بالمنشأة عاملاً مساعداً في كسب تأييد السكان وتعزيز وعيهم بأهمية المنشأة، مما ينعكس إيجاباً على مستوى الأمن الوقائي."12"

تأمين المداخل ونقاط التفتيش

تُعد المداخل ونقاط التفتيش بمثابة القلب النابض لمنظومة الأمن الوقائي في أي منشـــأة حيوية، فهي تمثل الواجهة الأولى التي تلتقي فيها إجراءات التحقق والتفتيش والمراقبة، وتشكل خط المواجهة الأول في مواجهة محاولات الاختراق أو التسلل. وتعتمد فعالية تأمين هذه النقاط على تكامل العناصـــر البشـــرية والتقنية والإجرائية، وعلى التخطيط الهندســـي المدروس الذي يراعي طبيعة المنشـــأة ونوع التهديدات المحتملة ومستوى التصنيف الأمني المطلوب."1"

تختلف مداخل المنشآت الحيوية وتنقسم تصنيفياً إلى ثلاثة أنواع رئيسية: المداخل الرئيسية المخصصة للعاملين والزوار، والتي تشهد كثافة مرورية عالية وتتطلب توازناً بين الإجراءات الأمنية وســـرعة الإنجاز؛ والمداخل الخدمية المخصـــصـــة للشاحنات والبضائع، والتي تتطلب أجهزة تفتيش متطورة وإجراءات صارمة نظراً لحجم البضـــائع وتنوعها؛ والمداخل الطارئة أو الاحتياطية التي تُفتح في حالات الضرورة القصوى وتخضع لإجراءات أمنية مشددة مع إبقائها مغلقة ومؤمنة في الظروف العادية. وقد يشمل التصنيف مداخل خاصة لكبار المسؤولين أو الشخصيات المهمة، تُجهز بمعايير أمنية مميزة وتخضـــع لإجراءات مختلفة تضـــمن حمايتهم مع مراعاة الجانب البروتوكولي. ويتم اختيار مواقع هذه المداخل بناءً على دراســـات أمنية وهندسية دقيقة، بحيث تُوضع بعيداً عن المناطق العمياء وتحت رقابة كاميرات المراقبة، مع توفير مســـافات أمان كافية تســـمح بالتعامل مع أي تهديد مفاجئ قبل وصوله إلى قلب المنشأة."2"

تعتمد المنشـــآت في تأمين مداخلها على مبدأ الدفاع المتدرج، الذي يقوم على تقســـيم عملية الدخول إلى مراحل متتابعة تزداد في صـــرامتها كلما اقترب الفرد أو المركبة من المنطقة الداخلية للمنشـــأة. ففي المرحلة الأولى وهي المحيط الخارجي، تُنشـــأ حواجز مادية وبوابات إلكترونية تعمل على إبطاء الحركة ومنع المركبات غير المصرح لها من الاقتراب، كما تُوضع لافتات تحذيرية وإرشادية لتوعية القادمين بالإجراءات المتبعة. وفي المرحلة الثانية وهي نقطة التفتيش الأولى، يُجرى التحقق

الأولي من الهوية والغرض من الزيارة، ويُفحص الأفراد والمركبات بصرياً باستخدام أجهزة كشف أساسية. أما المرحلة الثالثة وهي نقطة التفتيش الرئيسية، فتتضمن إجراءات تفتيش دقيقة باستخدام الأجهزة المتطورة، وتسجيل البيانات كاملة، وربطها بأنظمة المراقبة الداخلية، مع إمكانية الاحتفاظ بصور وبيانات للرجوع إليها عند الحاجة. وتأتي المرحلة الرابعة وهي الدخول إلى المنطقة الداخلية، حيث يُسمح بالدخول بعد استكمال الإجراءات، ويُوجَّه الفرد أو المركبة عبر مسارات محددة لا تتيح الوصول العشوائي إلى كافة مرافق المنشأة. وتُصمم مسارات الحركة الداخلية لضمان الفصل بين حركة المشاة والمركبات، وتقليل نقاط الالتقاء التي قد تشكل فرصاً أمنية أو حوادث تشغيلية."3"

المتطلبات التقنية لتأمين المداخل ونقاط التفتيش

يمثل الجانب التقني العمود الفقري لعملية تأمين المداخل، ويشمل مجموعة من الأنظمة والأجهزة التي تتكامل لتوفير تغطية أمنية شاملة. وتبرز في مقدمتها أنظمة كشف المعادن، والتي تتنوع بين البوابات الثابتة المثبتة عند المداخل الرئيسية، والأجهزة المحمولة باليد المستخدمة في التفتيش التفصيلي للأفراد، وأجهزة المسح بالأشعة السينية المخصصة للحقائب والطرود، وأجهزة الكشف عن المتفجرات والمخدرات في المركبات والبضائع. وتستند هذه الأجهزة إلى تقنيات متطورة كالمقاومة المغناطيسية والتصوير بالأشعة السينية والتحليل الطيفي، وتخضع لمعايير دقيقة في التشغيل والصيانة والدقة."4"

وتُعد أنظمة التحقق من الهوية عنصراً حيوياً آخر، وتتضمن أجهزة قراءة البطاقات الذكية والمفاتيح الإلكترونية، وأنظمة التعرف على بصمات الأصابع ومسح شبكية العين، وأجهزة التعرف على الوجه بالتقنيات الحرارية والثلاثية الأبعاد، وأنظمة التحقق متعددة العوامل التي تجمع بين أكثر من أسلوب تحقق لرفع مستوى الأمان، وتقنيات التحقق البيومتري عن بُعد التي تسمح بالمصادقة دون تلامس. وقد شهدت هذه الأنظمة تطوراً كبيراً في السنوات الأخيرة، خاصة مع إدخال تقنيات الذكاء

الاصـطناعي في تحليل الصـور البيومترية ومقارنتها بقواعد البيانات، مما زاد من دقة وسرعة عملية التحقق مع تقليل نسبة الأخطاء."5"

كما تشمل المتطلبات التقنية أنظمة المراقبة والتسجيل، التي تضم كاميرات المراقبة عالية الدقة المزودة بتقنيات الرؤية الليلية والتصـوير الحراري، وأجهزة تسـجيل الدخول والخروج بواسـطة البطاقات أو القياسـات الحيوية، وأنظمة تحليل الصـور بالفيديو لكشف السلوكيات المشبوهة، وأنظمة الأرشفة الرقمية للبيانات والصور لمدة زمنية كافية تتيح العودة إليها عند التحقيق في الحوادث. وتتكامل هذه الأنظمة مع أنظمة الاتصـال الداخلي والإنذار لضـمان سـرعة التبليغ عن أي حالة طارئة، ومع أنظمة التحكم المركزي التي تتيح الإشـراف على جميع العمليات من غرفة تحكم واحدة."6"

المتطلبات البشرية والإجرائية لتأمين المداخل

لا يمكن أن تؤدي المتطلبات التقنية وظيفتها بكفاءة دون توافر العنصـر البشـري المؤهل، الذي يقوم على تشـغيلها وصـيانتها واتخاذ القرارات المناسـبة بناءً على مخرجاتها. فطاقم الأمن المكلف بتأمين المداخل يحتاج إلى تدريب متخصـص ومستمر في عدة مجالات، منها التشغيل السليم لأجهزة التفتيش والمراقبة، وقدرات الملاحظة والكشـف عن التصـرفات المشـبوهة أو العلامات الدالة على الخطر، ومهارات التواصل الفعال مع مختلف فئات المترددين على المنشأة، والتأهيل النفسي للتعامل مع الحالات الحرجة والضـغوط الأمنية، والمعرفة الإجرائية بالقوانين والصلاحيات الممنوحة لهم. ويُوصـى أن يخضـع أفراد الأمن لتدريبات دورية على سـيناريوهات متنوعة، تشـمل حالات إنذار كاذبة، ومحاولات اختراق، وعمليات تسـلل، وهجمات إلكترونية، وتهديدات إرهابية، لضـمان اكتسـابهم الخبرة الميدانية اللازمة للتعامل مع مختلف الاحتمالات."7"

وتشـمل المتطلبات الإجرائية مجموعة من البروتوكولات المكتوبة والمُحدثة باسـتمرار، مثل بروتوكولات التعامل مع الزوار والمقاولين التي تنظم مراحل الاستقبال والتسجيل والتفتيش والمرافقة والخروج، وبروتوكولات التعامل مع حالات

الرفض أو المنع من الدخول وكيفية إبلاغ الشـــخص المعني بالقرار ولجانه في حال الاعتراض، وإجراءات التعامل مع المواد الممنوعة أو الخطيرة التي يتم ضـــبطها، وسياسات الخصوصية وحماية البيانات التي تضمن عدم إساءة استخدام المعلومات الشخصية، إلى جانب إجراءات الإبلاغ عن المخالفات والحوادث الأمنية وتسجيلها في ســـجلات مخصـــصـــة. وتخضـــع هذه الإجراءات للمراجعة الدورية للتأكد من ملاءمتها وفعاليتها في مواجهة التطورات الأمنية المســـتمرة، ويُشـــرك في هذه المراجعة جميع الأطراف المعنية من أفراد الأمن والإدارة والجهات الاســـتشـــارية "8".

تصميم نقاط التفتيش وتوزيعها

يُعد التصميم الهندسي لنقاط التفتيش عنصراً حاسماً في نجاح عملية تأمين المداخل، حيث يجب أن يضـمن تحقيق عدة أهداف في آن واحد: تحقيق الأمن بمنع النفاذ غير المصـــرح به، والســـرعة في إنهاء إجراءات الدخول لتجنب التكديس والتأخير، وسهولة الاستخدام للعاملين والزوار، مع إمكانية التوسع مستقبلاً واستيعاب الزيادة في الحركة. ويجب أن تشـتمل نقطة التفتيش جيدة التصـميم على مناطق محددة لكل وظيفة، كمنطقة وقوف للتفتيش الأولي، ومنطقة تسـجيل وتحقق من الهوية، ومنطقة تفتيش دقيق بالأجهزة، ومنطقة انتظار للحالات المســـتثناة، إلى جانب منفذ للخروج الآمن لحالات الطوارئ، وغرفة تحكم صـــغيرة للإشـــراف المباشـــر على العملية. وتُصـــمم هذه المناطق بحيث تسـمح بمرور الأشـخاص والمركبات في اتجاه واحد، وتفصـل بين المسـارات المختلفة لتجنب التداخل، وتوفر مخارج طوارئ بديلة يسـهل الوصول إليها في حالات الإخلاء المفاجئ."9"

كما يتم توزيع نقاط التفتيش وفق خطـة مدروســـة تراعي كثافة الحركة المتوقعة ومسـتوى التهديد لكل مدخل، حيث تُخصـص النقاط الرئيسـية لأكبر قدر من الحركة وتُزود بـأحدث التقنيـات، بينمـا تُســـتخدم نقـاط أقل تجهيزاً للمـداخل ذات الحركـة المحدودة. ويُنشـــأ عادةً نقطة تفتيش مركزية رئيســـية للموظفين الدائمين، وأخرى للزوار والمراجعين، وثالثة للشـــاحنات والبضـــائع، مع إمكانية وجود نقاط نوعية

للشخصيات المهمة أو للدخول في أوقات الطوارئ. وتُحدد ساعات العمل لكل نقطة بناءً على أنماط الحركة ونوعية النشـــاط في المنشـــأة، مع إمكانية التعديل في أوقات الذروة أو الأحداث الاستثنائية."10"

التعامل مع الحالات الاستثنائية والطوارئ عند نقاط التفتيش

تتطلب الطبيعة الأمنية لعمل نقاط التفتيش اســـتعداداً دائماً للتعامل مع الحالات الاســـتثنائية التي قد تطرأ بشـــكل مفاجئ، مثل محاولات الاقتحام بالقوة أو التســـلل باســـتخدام وثائق مزورة. وفي مثل هذه الحالات، يجب أن تكون لدى رجال الأمن إجراءات محددة ومتدربة تضمن سرعة الاستجابة دون التسبب في حالة من الذعر أو الفوضى، وتشمل تفعيل نظام الإنذار الداخلي، وعزل نقطة التفتيش وإغلاقها لمنع دخول أو خروج أي شخص، والاتصال الفوري بغرفة العمليات المركزية والجهات الأمنية المختصة، واتخاذ إجراءات التوقيف المؤقت للمشتبه بهم مع مراعاة الجوانب القانونية والإنسانية، مع توثيق الحادثة بكامل تفاصيلها لتكون مرجعاً في التحقيقات القادمة. كما قد تنشأ حالات طارئة بسبب حوادث فردية كإصابة أحد المترددين أو تعطل الأجهزة التقنية أو اندلاع حريق، الأمر الذي يتطلب وجود خطط بديلة وسريعة للتعامل مع كل حالة، وخطة إخلاء لنقطة التفتيش نفسها للحفاظ على سلامة الأفراد في الموقع."11"

ويشـــمل الاســـتعداد للطوارئ إجراء تدريبات عملية دورية تحاكي ســـيناريوهات متنوعة، كحالات الهجوم المسلح، والتهديد بقنبلة، والحرائق، والتسربات الكيميائية، والانقطاع الكامل للتيار الكهربائي وتعطل أنظمة التشغيل. وتُقيّم نتائج هذه التدريبات بدقة لتحديد مواطن القوة والضـــعف، وتُعدل الإجراءات والخطط بناءً عليها، مما يضمن تحسين الأداء بشكل مستمر ورفع مستوى الجاهزية لأي طارئ. كما ينبغي أن تتضمن خطط الطوارئ آليات للتواصل مع وسائل الإعلام وإدارة الرأي العام، لمنع انتشار الإشاعات والحفاظ على سمعة المنشأة ومصداقيتها في الأوقات الحرجة ."12"

كاميرات المراقبة وأجهزة الإنذار

تمثل كاميرات المراقبة وأجهزة الإنذار العمود الفقري لأنظمة الأمن الإلكتروني في المنشآت الحيوية، حيث تؤديان وظيفة متكاملة تقوم على الرصد المستمر والكشف المبكر عن أي خرق أمني أو حالة طارئة. وتتضافر هاتان التقنيتان لتشكيل نظاماً أمنياً يستشعر التهديدات لحظة وقوعها، ويمنح الجهات المسؤولة فرصة ثمينة للاستجابة قبل أن تتفاقم الأوضاع، مما يجعلهما من الأدوات الأكثر تأثيراً في إجراءات الأمن الوقائي."1"

أولاً: كاميرات المراقبة (الدوائر التلفزيونية المغلقة)

تشكل أنظمة كاميرات المراقبة ما يُعرف بالدوائر التلفزيونية المغلقة(CCTV) ، وهي وسيلة بصرية تتيح المراقبة المباشرة والمستمرة لكافة أرجاء المنشأة وأحيازها الحيوية، وتزود غرفة العمليات المركزية بتدفق حي للصور والفيديوهات. وقد تطورت هذه الأنظمة تطوراً هائلاً في السنوات الأخيرة، متجاوزة مجرد تسجيل الصور إلى تحليلها واستخلاص المعلومات منها تلقائياً بفضل تقنيات الذكاء الاصطناعي والتعلم الآلي."2"

وتتنوع كاميرات المراقبة من حيث النوع والمواصفات لتناسب مختلف الاحتياجات الأمنية والمكانية. فمن حيث التكنولوجيا، تُصنف إلى كاميرات تمثيلية وهي النوع التقليدي الذي يعمل بإشارات تناظرية، وكاميرات رقمية (IP) تنقل الصور عبر شبكة الإنترنت وتتيح جودة أعلى وتحكماً أكبر، وكاميرات تعمل بالأشعة تحت الحمراء للرؤية الليلية في الظلام الدامس، وكاميرات تصوير حراري تكشف عن وجود الأشخاص حتى في ظروف الضباب أو الدخان، وكاميرات بانورامية ذات زوايا رؤية واسعة لتغطية مساحات كبيرة، وكاميرات متحركة (PTZ) يمكن توجيهها عن بعد وتكبير الصورة وتدويرها. أما من حيث شكل التثبيت، فتتوفر كاميرات ثابتة مثبتة في مواقع محددة، وكاميرات متحركة مثبتة على أذرع دوارة، وكاميرات محمولة صغيرة الحجم للاستخدام المؤقت أو المتنقل، إلى جانب كاميرات

خفية تستخدم في المهمات الاستخبارية أو السرية للحصول على معلومات من دون إثارة الانتباه."3"

وتعتمد فعالية نظام المراقبة على التوزيع المدروس للكاميرات بحيث تغطي كافة النقاط العمياء والمناطق الحساسة. ويشمل التوزيع النموذجي وضع كاميرات عند جميع المداخل والمخارج، ونقاط التفتيش الرئيسية والفرعية، والممرات والمناطق المشتركة، ومحيط الأسوار الخارجية ومناطق العزل الأمني، والمرافق الحيوية كغرف المولدات والمحولات والمختبرات ومخازن المواد الخطرة، والمواقف والمناطق المكشوفة، إضافة إلى غرف التحكم والمرافق الإدارية الحساسة. وتُراعى في اختيار مواقع الكاميرا عدة معايير تقنية، كزاوية الرؤية التي تحدد مساحة التغطية، وعمق الميدان الذي يضمن وضوح الصور على مختلف المسافات، والإضاءة المتوفرة في الموقع وحاجته لكاميرات ليلية، وإمكانية توصيل الكاميرا بشبكة الطاقة والبيانات، فضلاً عن حمايتها من العوامل الجوية والبيئية كالغبار والرطوبة ودرجات الحرارة المتطرفة."4"

وفي المستوى المتقدم من التشغيل، تُدمج أنظمة المراقبة مع برمجيات تحليل الفيديو الذكية(Video Analytics) ، التي تتيح ميزات متطورة ككشف الحركة غير المصرح بها في المناطق المحظورة، وتتبع حركة الأشخاص والمركبات وتحديد مساراتها، والتعرف على الوجوه ومقارنتها بقواعد البيانات المطلوب أمنياً، وكشف الأشياء المتروكة أو المشبوهة، وكشف تجاوز الحدود الجغرافية الافتراضية (المسيجات الإلكترونية)، ورصد حالات الجري أو السلوك العدواني، وتحليل الكثافات المرورية واكتشاف الاختناقات. وهذه الميزات لا تعزز الكشف المبكر فحسب، بل تقلل من الأخطاء البشرية وتوفر جهداً كبيراً في عمليات المراقبة."5"

ثانياً: أجهزة الإنذار

تعمل أجهزة الإنذار كحاسة سادسة للمنشأة، تتنبه إلى المخاطر في مهدها وتبلغ عنها قبل أن تتسبب في أضرار جسيمة. وتتنوع هذه الأجهزة وفقاً لنوع الخطر الذي تكشفه، ويُصنف كل منها بتقنيات واستخدامات محددة تتناسب مع التهديدات

المختلفة. ومن أبرز هذه الأجهزة أجهزة كشف التسلل للمحيط، والتي تشمل أجهزة استشعار الاهتزاز المثبتة على الأسوار، وأجهزة الكشف بالأشعة تحت الحمراء السلبية (PIR) التي ترصد تغيرات الحرارة الناجمة عن حركة الأجسام، وأجهزة الميكروويف والموجات فوق الصوتية التي تخلق حقلاً كهرومغناطيسياً وتكشف أي اختراق له، وأجهزة الكشف بالخيوط أو الأسلاك المتوترة التي تنبه عند قطعها. أما أجهزة كشف الحريق والدخان فتعتمد على تقنيات التأين والضوء المشتت، وتتصل مباشرة بأنظمة إطفاء الحرائق الآلية."6"

وتشمل أجهزة الإنذار أيضاً أنظمة كشف الغازات والمواد الخطرة كأجهزة كشف أول أكسيد الكربون والميثان وكبريتيد الهيدروجين، وأجهزة الكشف عن التسربات الإشعاعية والكيميائية، وأجهزة قياس مستوى الأكسجين في الأماكن المغلقة. وهناك أنظمة متخصصة لكشف السوائل القابلة للاشتعال والمتفجرات، وكاشفات المعادن الثابتة والمحمولة. وتكتمل المنظومة بأنظمة الإنذار اليدوية التي تسمح للأفراد بالتبليغ عن الحوادث عند اكتشافها، بالإضافة إلى أنظمة الاتصال الصوتي للإنذار الجماعي كصفارات الإنذار ومكبرات الصوت للطوارئ، وأنظمة الإنذار الإلكترونية التي ترسل رسائل نصية وإشعارات فورية للمسؤولين."7"

وتعتمد فاعلية نظام الإنذار بشكل كبير على آلية الربط والتشغيل، حيث تُربط جميع الأجهزة بغرفة تحكم مركزية تتلقى الإشارات، وتصنفها وفق مستوى الخطورة (تنبيه، خطر محدود، خطر داهم، حالة كارثة)، ثم تحولها إلى استجابة مناسبة. كما تُجهز هذه الأنظمة بأنظمة طاقة احتياطية لضمان استمرار عملها في حالات انقطاع التيار الرئيسي، وتخضع لاختبارات دورية للتأكد من سلامة أدائها، ويُوثق كل إنذار بوقته ونوعه وموقعه وطريقة التعامل معه للاستفادة منها مستقبلاً."8"

ثالثاً: التكامل بين أنظمة المراقبة والإنذار

لا يتحقق الأمن الإلكتروني المثالي في المنشآت الحيوية إلا من خلال التكامل العضوي بين كاميرات المراقبة وأجهزة الإنذار، بحيث تشكل المنظومة كلاً واحداً يؤدي وظيفة متسقة ومتكاملة. فعندما يُطلق جهاز إنذار أي إشارة خطر، تُوجه

الكاميرات الموجودة في المنطقة تلقائياً لتسجيل ما يحدث وتقديم صورة حية لغرفة العمليات، مما يمكن المشغلين من تحديد نوع الخطر بدقة وتقييم حجمه قبل اتخاذ القرار المناسب. وهذا التكامل يتيح أيضاً ربط الإنذار بتسجيل الفيديو، بحيث يبدأ التسجيل التلقائي فور إطلاق الإنذار لتوثيق الحدث، ويُمكن الرجوع إليه لاحقاً للتحقيق وإثبات الوقائع."9"

ويتجاوز هذا التكامل الإجراءات التفاعلية إلى المستوى التكاملي الاستباقي، حيث تُبرمج أنظمة التحليل الذكي للكاميرات لتنبه ذاتياً عند ملاحظة سلوكيات تنذر بحدوث خطر، كتجاوز الأفراد للمناطق المحظورة أو ترك حقائب مشبوهة، دون حاجة إلى تفعيل إنذار مادي. وهذا النوع من التكامل الذكي يُعزز قدرة المنشأة على كشف التهديدات قبل وقوعها ويوفر وقتاً ثميناً للاستباق، مما يجعله نقلة نوعية في إجراءات الأمن الوقائي المعاصر."10"

رابعاً: الاعتبارات التنظيمية والقانونية لتشغيل أنظمة المراقبة والإنذار

يخضع استخدام كاميرات المراقبة وأجهزة الإنذار في المنشآت الحيوية لضوابط تنظيمية وقانونية صارمة، تهدف إلى تحقيق التوازن بين متطلبات الأمن وحماية خصوصية الأفراد. وتتضمن هذه الاعتبارات ضرورة الحصول على التراخيص اللازمة من الجهات المختصة لتركيب أنظمة المراقبة في الأماكن العامة وشبه العامة، وإخطار العاملين والزوار بوجود كاميرات مراقبة عبر لافتات واضحة في المداخل والأماكن المكشوفة، والالتزام بعدم وضع كاميرات في الأماكن التي تمس بالخصوصية كدورات المياه وغرف تغيير الملابس. كما تشمل حماية البيانات المسجلة من الوصول غير المصرح به، وتحديد صلاحيات الاطلاع على التسجيلات بما يضمن عدم إساءة استخدامها، وفترات احتفاظ محددة بالتسجيلات وفقاً للتشريعات الوطنية، وإتاحة التسجيلات للجهات القضائية والأمنية عند الطلب الرسمي."11"

وتتضمن القوانين عادةً أحكاماً بشأن الإفصاح عن نظام المراقبة لجميع الأطراف المعنية، وضوابط استخدام التسجيلات في التحقيقات الداخلية والخارجية، وعقوبات

على مخالفة هذه الضـــوابط. كما تلزم بعض التشـــريعات المنشـــآت الحيوية بتعيين مســؤول لحماية البيانات يتولى الإشــراف على الامتثال لهذه المتطلبات والتبليغ عن أي خروقات محتملة، مما يضـــفي طابعاً مؤســـســـياً وجاداً على إدارة هذا الجانب الحساس من العمليات الأمنية."12"

أسوار وبوابات المنشآت

تمثل الأسوار والبوابات العنصر المادي الأكثر وضوحاً في منظومة الأمن الوقائي للمنشآت الحيوية، حيث تشكل الحاجز المادي الأول الذي يفصل بين البيئة الداخلية للمنشأة والمحيط الخارجي. ولا تقتصر وظيفتها على الجانب المادي في منع أو تأخير النفاذ غير المصرح به، بل تمتد لتشمل أدواراً ردعية ونفسية، إذ ترسل إشارة واضحة إلى المترددين والمارة حول طبيعة المنشأة ومستوى الحماية المطبقة فيها. ويعتمد تصميم الأسوار والبوابات وتنفيذها على تقييم دقيق للمخاطر، وطبيعة التهديدات المحتملة، والمستوى الأمني المطلوب، والظروف البيئية والجغرافية المحيطة."1"

أولاً: الأسوار الأمنية (أنواعها ومواصفاتها)

تتنوع الأسوار الأمنية المستخدمة في تأمين المنشآت الحيوية بحسب متطلبات الحماية ومستوى التهديد، ويمكن تصنيفها بشكل رئيسي إلى أسوار خرسانية، وأسوار معدنية، وأسوار كهربائية وإلكترونية، وأسوار طبيعية أو مختلطة. وتتميز الأسوار الخرسانية بقوتها الهيكلية العالية وقدرتها على مقاومة محاولات الاقتحام بالمركبات أو الأدوات الثقيلة، وتُستخدم عادةً للمنشآت ذات التصنيف الأمني الأعلى كالسجون والمراكز الحكومية الحساسة والمنشآت النووية والعسكرية، وقد تُزود هذه الأسوار بقنوات للأسلاك الشائكة أو أنظمة كشف الاهتزاز لتعزيز فعاليتها. أما الأسوار المعدنية (الشبكية أو الحديدية) فتُعد من أكثر الأنواع شيوعاً لتوازنها بين التكلفة والفعالية، وتتنوع في أشكالها كالشبك المنسوج، والقضبان العمودية، والألواح المعدنية المثقبة، وتُستخدم على نطاق واسع في المنشآت الصناعية والتجارية والمطارات، وغالباً ما تُرفع فوقها أسلاك شائكة أو شرائط حادة لردع محاولات التسلق."2"

وتشمل الأسوار الكهربائية والإلكترونية فئة متطورة تجمع بين الحاجز المادي وتقنيات الصعق الكهربائي أو أنظمة الكشف الذكية، وهي تستخدم في المنشآت ذات الحساسية القصوى كالمناطق العسكرية المحظورة والمرافق النووية، إذ تعمل على

ردع المتسللين وإصدار إنذار فوري لدى ملامستها. أما الأسوار الطبيعية أو المختلطة فتستفيد من المعالم الجغرافية كالأنهار والمنحدرات والتضاريس الوعرة، وتُدمج مع حواجز صناعية لتشكيل نظام دفاعي متكامل، وتستخدم غالباً في المنشآت الواقعة في مناطق نائية أو ذات تضاريس متنوعة. وتتميز الأسوار الأمنية النموذجية بارتفاع يتناسب مع مستوى التهديد، وغالباً ما يتراوح بين ٢,٥ متر في المنشآت المتوسطة إلى ٥ أمتار أو أكثر في المنشآت عالية المخاطر، مع تصميم يمنع التسلق بواسطة الأسطح الملساء أو المائلة أو الإضافات المانعة كالشائك الحلزوني والشرائط الحادة."3"

ثانياً: المعايير الفنية للأسوار الأمنية

تخضع الأسوار الأمنية المصممة للمنشآت الحيوية لمجموعة من المعايير الفنية والهندسية الدقيقة، تهدف إلى ضمان تحقيق المستوى المطلوب من الحماية مع مراعاة عوامل الاستدامة وسهولة الصيانة. ومن أبرز هذه المعايير معيار الارتفاع، حيث يُنصح بأن لا يقل عن ٢,٥ متر للمنشآت المتوسطة، في حين يتطلب الأمن المشدد ارتفاعات تصل إلى ٤ أمتار فأكثر مع إضافة أذرع مانعة للتسلق. ويُعد معيار السماكة والمتانة أمراً بالغ الأهمية، إذ يجب أن تكون المواد المستخدمة قادرة على مقاومة محاولات القطع أو الاقتحام لفترة زمنية كافية تتيح للاستجابة الأمنية الوصول، وتستخدم في هذا السياق سبائك فولاذية عالية الجودة أو الخرسانة المسلحة بمواصفات خاصة. ويشمل المعيار أيضاً عمق الأساسات، لضمان ثبات السور ومنع اختراقه من الأسفل بالحفر، وغالباً ما يُدفن جزء من السور تحت سطح الأرض ليمنع الحفر تحته."4"

وتتطلب الأسوار عالية الأداء أنظمة كشف مدمجة، كأجهزة استشعار الاهتزاز أو التوتر التي تُثبت على جسم السور لترصد أي محاولة تسلق أو قطع أو اهتزاز غير طبيعي، وتُربط مباشرة بغرفة التحكم لتفعيل الإنذار الفوري. وتُعد الإضاءة الكافية على طول خط السور معياراً أساسياً لضمان الرؤية الليلية ودعم عمل كاميرات المراقبة، وتُستخدم عادةً أضواء LED عالية الكثافة موزعة بانتظام على طول

المحيط. كما يُراعى في التصـــميم منع وجود نقاط عمياء أو مناطق يمكن أن تخفي متسللاً، من خلال تصميم السور بشكل مستقيم أو بتدويرات مدروسة، وتوفير مسافة أمان خالية من المزارع أو المباني خارج الســـور. وتُحدد هذه المعايير غالباً في وثائق معايير وطنية أو دولية كتلك الصـــادرة عن المنظمة الدولية للمعايير أو الوكالات الأمنية المتخصصة."5"

ثالثاً: بوابات المنشآت (أنواعها وتصميمها)

تُمثل البوابات نقاط الضـعف المحتملة في محيط المنشـأة، إذ يتعين فيها فتح المجال لدخول الأفراد والمركبات مع الحفاظ على المسـتوى الأمني المطلوب. ولذلك، يُولى تصـميم البوابات واختيار أنواعها عناية خاصـة تضـمن تحقيق التوازن بين الأمن والسـلاسـة التشـغيلية. وتصـنف البوابات الأمنية حسـب حجمها وطريقة تشـغيلها ومستوى حمايتها إلى عدة أنواع رئيسية: البوابات المفصلية التي تفتح بشكل تقليدي وتستخدم للمداخل الصغيرة والمشاة، والبوابات المنزلقة التي تنزلق جانبياً وتستخدم للمداخل الكبيرة ذات الحركة المرورية العالية، والبوابات المتدحرجة التي تتحرك على قضـــبان أرضـــية، والبوابات المتأرجحة على محور مركزي، والبوابات الكهربائية الأوتوماتيكية التي تُفتح وتُغلق عن بعد، والبوابات المدرعة المصـــممة لمقاومة الرصاص والانفجارات في المنشآت عالية المخاطر."6"

وتُجهز البوابات الحديثة بأنظمة تحكم متطورة تشـــمل أجهزة قراءة البطاقات أو القياســـات الحيوية للتحقق من هوية الراغبين في الدخول، وكاميرات مراقبة موجهة لتســـجيل كافة عمليات الدخول والخروج وأصـــحابها، وأجهزة كشـــف المعادن والمتفجرات المثبتة على البوابة نفسـها، وأنظمة اتصـال صـوتي ومرئي مع غرفة العمليات، ومصادر طاقة احتياطية تعمل في حالات انقطاع التيار الكهربائي، وآليات فتح طارئ يدوية للاسـتخدام في حالات الطوارئ أو عند تعطل الأنظمة الكهربائية. وتختلف درجة تجهيز البوابة بحســـب أهميتها وتصـــنيفها الأمني، وتكون البوابات الرئيسية عادةً الأكثر تجهيزاً وتكاملاً من الناحية التقنية."7"

رابعاً: المناطق العازلة والحواجز الأمنية المساندة

إلى جانب الأسوار والبوابات الرئيسية، تُستخدم مناطق عازلة وحواجز أمنية مساندة لتعزيز فعالية الحماية المحيطية، خاصة في المنشآت المعرضة لهجمات بالمركبات أو القنابل. وتشمل هذه المناطق ما يُعرف بالمنطقة العازلة، وهي مساحة فارغة بين السور الخارجي والمباني الداخلية للمنشأة، تهدف إلى إبطاء أي اختراق وإعطاء فرصة للاستجابة، وتُزرع أحياناً بأشجار أو تُزود بعوائق طبيعية. وتندرج ضمنها الممرات الأمنية التي تسمح بدوريات المشاة أو المركبات الخفيفة على طول السور الداخلي، وتُستخدم فيها أجهزة كشف الحركة والحواجز الأرضية لضمان السيطرة الكاملة على المحيط. أما الحواجز المانعة لاقتحام المركبات فتشمل الحواجز الخرسانية) كالحواجز على شكل حرف(NJ ، والأعمدة القابلة للرفع والطيّ (البولاردات)، والحواجز الشبكية الممتدة، وصناديق الرمل أو الماء المُعبأة، والسياجات القابلة للطي في حالات الطوارئ، وتوضع عادةً عند المداخل الرئيسية ونقاط التفتيش لمنع اقتحام المركبات بسرعة عالية."8"

ويزداد التعقيد الأمني في بوابات دخول المركبات، حيث تُنشأ غالباً "غرف احتجاز" أو "مصائد" تسمح بدخول مركبة واحدة في كل مرة وإخضاعها للتفتيش قبل فتح البوابة الداخلية، مما يمنع تدفقاً غير مراقب ويصعّب على أي جهة معادية اختراق البوابة بقوة. وتُستخدم في هذه الغرف كاميرات متعددة الزوايا، وأجهزة مسح للهيكل السفلي للمركبة، وأنظمة كشف للمواد المشبوهة، مما يُشكل حاجزاً أمنياً مزدوجاً يعزز الأمن ويضاعف من صعوبة الاختراق."9"

خامساً: اعتبارات الصيانة والتقييم الدوري للأسوار والبوابات

تتعرض الأسوار والبوابات لعوامل تآكل وتلف متعددة تشمل العوامل الجوية (كالأمطار والرطوبة والحرارة الشديدة والرياح المحملة بالأتربة)، وعوامل الاستخدام اليومي المتكرر للبوابات، ومحاولات التخريب أو العبث، وتقادم الأنظمة الإلكترونية المرتبطة بها، ونمو النباتات حول الأساسات أو قرب الأسوار مما قد يسهل التسلق أو يُعيق عمل الكاميرات. ولذلك، فإن الصيانة الدورية والتقييم المستمر لهذه العناصر يُعد جزءاً لا يتجزأ من الإجراءات الوقائية، ويشمل ذلك فحصاً دورياً

منتظماً لهيكل السور والبوابات للكشف عن أي تصدعات أو تآكل أو أعطال، واختباراً لأنظمة الكشف والإضاءة والتحكم الإلكتروني للتأكد من عملها بكفاءة، وتشحيم المكونات الميكانيكية للبوابات وضبط محركاتها، وإزالة أي عوائق أو نباتات حول الأسوار، إلى جانب تحديث الأنظمة التقنية المرتبطة بالبوابات عند توفر تقنيات أحدث. ويُوصى بأن تجرى عمليات التقييم الأمني الشامل للأسوار والبوابات بشكل دوري من قبل خبراء مستقلين، مع إعادة تقييم المخاطر كلما طرأت تغيرات على طبيعة المنشأة أو محيطها أو مستوى التهديدات الموجهة إليها."10"

سادساً: الاعتبارات البيئية والجمالية في تصميم الأسوار والبوابات

لا يقتصر تصميم الأسوار والبوابات على الجوانب الأمنية والتقنية فحسب، بل يتضمن أيضاً مراعاة الاعتبارات البيئية والجمالية التي تضمن اندماج المنشأة مع محيطها الطبيعي والحضري، وتحقق قبولاً اجتماعياً أوسع دون الإخلال بالمتطلبات الأمنية. ويمكن تحقيق ذلك من خلال اختيار ألوان وتشطيبات تتناسب مع البيئة المحيطة وتقلل من المظهر القاسي للحواجز الأمنية، واستخدام مواد تسمح بالرؤية من خلالها كالشبك المعدني المطلي بدلاً من الجدران الخرسانية الصماء، وتنسيق المساحات الخضراء والأشجار حول الأسوار بطريقة لا تُعيق الرقابة الأمنية، وتصميم البوابات بأشكال معمارية تتناسب مع الهوية البصرية للمنشأة. وتزداد أهمية هذه الاعتبارات في المنشآت الموجودة في المناطق السكنية أو ذات القيمة التاريخية أو الجمالية، إذ تُسهم في تقليل الاحتكاك مع السكان المحليين وتعزيز صورة المنشأة كجزء من النسيج المجتمعي لا كحصن منعزل، مع الحفاظ على المستوى الأمني المطلوب. وقد أثبتت الدراسات أن تحسين المظهر الجمالي للأسوار والبوابات يسهم في رفع الروح المعنوية للعاملين وزيادة الشعور بالانتماء، كما يقلل من الاستفزاز الذي قد تشعر به بعض الجهات المعادية تجاه المنشآت ذات المظهر العسكري المفرط."11"

وتؤدي الأسوار والبوابات في المنشآت الحيوية دوراً يتجاوز كونها مجرد حواجز مادية، فهي عناصر تشغيلية حية في منظومة الأمن الوقائي تتفاعل مع أنظمة

المراقبة والإنذار والتحكم، وتشكل معاً كياناً أمنياً متكاملاً. ويقتضي التصميم الناجح لهذه العناصر تكامل الخبرات الهندسية والأمنية والإدارية، مع مراعاة التوسع المستقبلي للمنشأة وقدرتها على استيعاب تقنيات أمنية جديدة، حيث أن أي تقصير في تصميمها أو صيانتها قد يُفشل منظومة الأمن بأكملها، مهما بلغت درجة تطور الأنظمة الأخرى."12"

إجراءات تأمين حرم المنشأة

يشير مصطلح حرم المنشأة إلى كامل المساحة الجغرافية المحددة التي تقع ضمن نطاق الملكية أو الولاية القانونية للمنشأة، وتمتد من الأسوار الخارجية إلى حدود المباني والمرافق الداخلية. ويُعد تأمين هذا الحرم من المهام الأمنية الشاملة التي تتجاوز مجرد حماية المداخل أو نقاط التفتيش، لتشمل مراقبة الأنشطة كافة داخل المحيط، وتنظيم الحركة، وحماية الأصول المادية والبشرية، وضمان استمرارية العمليات الحيوية. وتقوم إجراءات تأمين الحرم على مبدأ الدفاع المتعمق، بحيث تُقسم المنطقة الداخلية إلى نطاقات أمنية متدرجة تزداد صرامة كلما اقتربنا من قلب المنشأة، مما يضمن احتواء أي خرق أمني ومنع انتشاره إلى المناطق الأكثر حساسية."1"

أولاً: تقسيم المناطق الداخلية وتصنيفها أمنياً

يُعد تقسيم حرم المنشأة إلى مناطق أمنية متباينة المستوى من الركائز الأساسية لتأمين الحرم، حيث يُمكن من توزيع الموارد الأمنية وفقاً للأولويات وتركيز الجهود على حماية الأصول الأكثر قيمة وحساسية. ويتبع هذا التقسيم عادةً نمطاً هرمياً يبدأ بالمناطق العامة (كالمداخل والمواقف والطرق الخارجية والمرافق الخدمية ذات الحركة العالية)، ثم المناطق المقيّدة (وهي المناطق التي يُسمح بالدخول إليها لفئات محددة من الموظفين بعد التحقق من صلاحياتهم، كالمكاتب الإدارية والممرات الداخلية والمختبرات غير الحرجة)، فالمناطق المحظورة (وهي المناطق شديدة الحساسية التي يُسمح فيها فقط لأفراد محددين بتفويضات أمنية خاصة، كغرف التحكم ومراكز البيانات ومخازن المواد الخطرة)، وأخيراً المناطق العازلة أو الآمنة تماماً (وهي المناطق الأكثر تحصيناً داخل المنشأة، كغرف العمليات السرية والمواقع النووية أو الكيميائية الحساسة)."2"

وتُصمم نقاط المراقبة والتحكم بين كل منطقة وأخرى لضمان عدم انتقال الأفراد أو المواد بينها دون إذن صريح، وتُركب أنظمة كشف متطورة عند الفواصل بين المناطق، ويُطبق مبدأ "الحد الأدنى من الصلاحيات" بحيث لا يحصل أي فرد إلا

على الصـلاحيات الضـرورية لأداء مهامه فقط. ويُسـهم هذا التقسـيم في احتواء أي حادث أمني ضمن المنطقة التي وقع فيها، ومنع امتداده إلى المناطق الأكثر حساسية، كما يُسـهل إجراءات الإخلاء الجزئي عند الحاجة دون تعطيل عمل المنشـأة بأكملها "3".

ثانياً: تنظيم حركة الأشخاص والمركبات داخل الحرم

تتطلب إدارة الحركة داخل حرم المنشـأة تخطيطاً هندسـياً وتنظيمياً دقيقاً يفصـل بين مسـارات المشـاة والمركبات ويضـمن انسـيابية الحركة دون تعارض مع المتطلبات الأمنية. ويشـمل ذلك تحديد مسـارات محددة لحركة المشـاة، وممرات للمركبات الخفيفة والثقيلة، ومناطق مخصـصـة لتحميل وتفريغ البضـائع بعيدة عن المباني الحيوية، ومواقف مصـنفة بحسـب الفئة والصـلاحية. كما تُوضـع لافتات إرشـادية واضحة تبين المناطق المسموح دخولها والمناطق الممنوعة، وتُستخدم أنظمة ملاحة إلكترونية في المنشآت واسعة النطاق لتوجيه الزوار والموظفين. ويُشترط في تنظيم الحركة أن يكون قابلاً للتعديل بحسـب الظروف الاسـتثنائية كحالات الطوارئ أو أعمال الصيانة أو الزيارات الرسمية رفيعة المستوى."4"

وتُعد إجراءات منع التجمعات غير المرخصـة داخل الحرم جزءاً أسـاسـياً من هذا التنظيم، حيث تُراقب تحركات الأفراد وتحلل أنماطها للكشـف عن أي سـلوك غير اعتيادي قد ينم عن نوايا غير مشـروعة. وتُسـتخدم كاميرات المراقبة الذكية وأنظمة تحليل الحركة لرصد الاختناقات المرورية أو التجمعات غير المألوفة، وإبلاغ غرفة العمليات لاتخاذ الإجراء المناسـب، سـواء بتوجيه الدوريات الأمنية أو إصـدار تعليمات بالتفرق أو إخلاء المنطقة مؤقتاً."5"

ثالثاً: أنظمة المراقبة المستمرة للحرم

تسـتند المراقبة المسـتمرة لحرم المنشـأة إلى شـبكة مترابطة من الكاميرات وأجهزة الاسـتشـعار وأنظمة التحليل الذكية، التي تغطي كافة أرجاء الحرم دون اسـتثناء، وتعمل على مدار السـاعة لتسـجيل وتحليل الأنشـطة. وتُوزع الكاميرات على ارتفاعات وزوايا مختلفة لضـمان تغطية شـاملة ومنع النقاط العمياء، وتُجهز بتقنيات

الرؤية الليلية والتصـوير الحراري لتوفير رؤية واضـحة في جميع الأحوال الجوية والإضـاءة. وتُدمج مع أنظمة التحليل الذكي التي تكتشـف التغيرات في المشـهد وتُعلم المشـغلين فوراً عند حدوث أي شـذوذ، كوجود شـخص في منطقة محظورة، أو ترك حقيبة مشـبوهة، أو تغيير مفاجئ في أنماط الحركة، أو محاولة التلاعب بالكاميرات أو العبث بمساراتها."6"

وتشـمل مراقبة الحرم أيضـاً أنظمة كشـف المحيط الداخلي التي تُوضـع على طول الممرات والمناطق الفاصـلة بين النطاقات الأمنية، كأجهزة كشـف الحركة بالأشـعة تحت الحمراء، وأجهزة الموجات فوق الصوتية، وكاشفات الاهتزاز على الأرضيات والنوافذ، وأجهزة كشـف الضـغط في الممرات الضـيقة. وتُربط هذه الأجهزة بغرفة التحكم لتُصدر إنذاراً فورياً لدى كشف أي تحرك غير مصرح به، مما يتيح استجابة سريعة وفعالة."7"

رابعاً: إجراءات الدوريات الأمنية داخل الحرم

لا يمكن للأنظمة الإلكترونية أن تحل محل العنصـر البشـري في تأمين الحرم، إذ تظل الدوريات الأمنية الميدانية عنصراً لا غنى عنه لتحقيق الحضور الأمني الفعلي والردع المباشـر. وتقوم هذه الدوريات بجولات منتظمة وغير مجدولة على كافة مرافق الحرم، وتتحقق من سـلامة الأبواب والنوافذ والأسـوار، وتتفقد العاملين وتطلب منهم إبراز الهويات عند الاقتضـاء، وترصـد أي مؤشـرات على سـلوكيات غير اعتيادية كالأصـوات العالية أو الروائح الغريبة أو بوادر الحرائق، وتسـتجيب للإنذارات والبلاغات فور ورودها. وتُوثق جولات الدوريات وتسـجل في سـجلات خاصـة، وتُحلل البيانات المجمعة لتحديد أنماط المخاطر المحتملة وتعديل خطط الدوريات وفقاً لذلك."8"

وتعتمد فعالية الدوريات على التخطيط المسبق لمساراتها بحيث تغطي كافة المناطق وفق أوقات متفاوتة، مع عنصر المفاجأة في توقيت الجولات لمنع التنبؤ بها، وتزويد أفراد الدوريات بأجهزة اتصـال متطورة تمكنهم من التواصـل الفوري مع غرفة العمليات، وأجهزة كشف محمولة كأجهزة كشف المعادن أو الغازات للاستخدام عند

الاقتضـــاء، مع الإلمام الكامل بخطط الطوارئ وإجراءات التعامل مع الحالات المختلفة."9"

خامساً: إجراءات التعامل مع الزوار والمقاولين داخل الحرم

تتطلب إدارة حركة الزوار والمقاولين داخل حرم المنشأة إجراءات صارمة تضمن عدم تحولهم إلى مصدر تهديد أمني، وتشمل تسجيلهم لدى نقطة التفتيش الرئيسية والتحقق من هوياتهم وصلاحياتهم، ومنحهم تصاريح دخول مؤقتة مزودة بتقنيات التتبع (كالبطاقات الذكية أو رموز الاستجابة السريعة أو تقنيات تحديد المواقع)، وتحديد المناطق المسموح لهم بدخولها ومنعهم من التجول بحرية خارجها، وتكليف مرافقين معتمدين لمرافقتهم في جولاتهم، ومنعهم من استخدام الكاميرات الشخصية أو أجهزة التسجيل داخل المناطق المقيّدة، ومصادرة التصاريح عند الانتهاء من الزيارة والتأكد من مغادرتهم للمنشأة. وتُسجل كافة تحركات الزوار والمقاولين في أنظمة المراقبة، وتُحلل هذه البيانات بشكل دوري للكشف عن أي أنماط مشبوهة أو تكرار غير مبرر لزيارات معينة."10"

سادساً: إجراءات الإخلاء والطوارئ داخل الحرم

يُعد التخطيط للإخلاء وإدارة الطوارئ جزءاً لا يتجزأ من إجراءات تأمين الحرم، إذ تضمن هذه الإجراءات سلامة الأفراد وحماية الأصول في حالات الطوارئ كالحرائق أو التسربات الكيميائية أو التهديدات الأمنية. وتشمل هذه الإجراءات وضع خطط إخلاء محدثة لكل منطقة من مناطق المنشأة، تحدد مخارج الطوارئ ونقاط التجمع الآمنة ومسارات الإخلاء، وتدريب العاملين على تنفيذها بانتظام، وتوزيع أجهزة إنذار يدوية وطفايات حريق وصناديق إسعافات في مواقع استراتيجية، وتخصيص فرق استجابة للطوارئ مدربة على التعامل مع مختلف السيناريوهات، إلى جانب تجهيز غرفة عمليات طوارئ منفصلة تتولى إدارة الأزمة وتنسيق الجهود مع الجهات الخارجية."11"

وتُجرى تدريبات إخلاء دورية بمشاركة جميع العاملين، وتُستخلص الدروس المستفادة من كل تدريب لتطوير الخطط والإجراءات، وتُوثق نتائجها في سجلات

خاصة تُستخدم كمرجع في عمليات التقييم الأمني المستمر. ويُعد التنسيق المسبق مع الجهات الخارجية كالدفاع المدني والإسعاف والشرطة عنصراً حيوياً، لضمان استجابة سريعة وفعالة عند وقوع الطوارئ الكبرى التي تتجاوز قدرات المنشأة الذاتية."12"

أنظمة الإغلاق والتحكم بالدخول

تمثل أنظمة الإغلاق والتحكم بالدخول الركيزة الإجرائية والتقنية التي تضـــمن عدم تمكين أي فرد من الوصـول إلى مرافق المنشـأة الحيوية أو مناطقها الداخلية إلا بعد اسـتيفائه للشـروط والصـلاحيات المقررة. وتعمل هذه الأنظمة كحلقة وصـل بين إجراءات التفتيش عند المداخل، وأنظمة المراقبة، وتصنيف المناطق الداخلية، لتشكل معاً منظومة متكاملة لإدارة الهوية والحركة داخل الحرم. وتستند فلسفة هذه الأنظمة إلى مبدأين أسـاسـيين: مبدأ "الحد الأدنى من الصـلاحيات" الذي يمنح كل فرد الصـلاحيات اللازمة لأداء مهامه فقط، ومبدأ "التسـجيل والتتبع" الذي يضـمن توثيق كل عملية دخول أو خروج لتصبح مرجعاً للتحقيق والمراجعة الأمنية."1"

أولاً: أنواع أنظمة التحكم بالدخول

تتنوع أنظمة التحكم بالدخول وفقاً لمسـتوى التأمين المطلوب وطبيعة الاسـتخدام، ويمكن تصنيفها إلى ثلاثة مستويات رئيسية: المستوى الأساسي القائم على المعرفة، والمسـتوى المتوسـط القائم على الحيازة، والمسـتوى المتقدم القائم على القياسـات الحيوية. فالمسـتوى الأول يشـمل أنظمة الأرقام السـرية والرموز الرقمية، وكلمات المرور البسـيطة، وأسـئلة التحقق الأمني، وتُسـتخدم عادةً للمناطق الأقل حسـاسـية كالمكاتب الإدارية العامة، وهي الأقل تكلفة ولكنها الأكثر عرضـــة للاختراق عبر التخمين أو المراقبة أو الإكراه. أما المســـتوى الثاني فيشـــمل البطاقات الممغنطة والبطاقات الذكية والمفاتيح الإلكترونية والمفاتيح القريبة (Proximity) والبطاقات التي تعمل بتقنية الترددات الراديوية(RFID) ، بالإضـــافة إلى الرموز المؤقتة التي تُرسـل عبر الهواتف المحمولة، وهو مسـتوى أكثر أمناً ويُسـتخدم للمناطق متوسـطة الحسـاسية، ولكنه يتطلب إدارة دقيقة للبطاقات ومنع فقدانها أو سرقتها. أما المستوى الثالث الأكثر تقدماً فيعتمد على القياسـات الحيوية كبصـمات الأصـابع والتعرف على الوجه ومسـح قزحية العين والتعرف على الصـوت وتحليل الأوردة، وهو المسـتوى المعتمد في المناطق شـديدة الحسـاسـية، إذ يصـعب تزويره ويوفر درجة عالية من الدقة، لكن تكلفته أعلى ويتطلب بنية تحتية تقنية متقدمة."2"

وتُســـتخدم في التطبيقات الأمنية المتطورة أنظمة التحقق متعددة العوامل(Multi-Factor Authentication)، التي تجمع بين مســتويين أو أكثر من المســتويات السابقة، كاشتراط البطاقة الذكية مع بصمة الإصبع، أو الرقم السري مع مسح شبكية العين، مما يرفع مستوى الأمان بشكل كبير ويجعل عملية الاختراق شبه مستحيلة. وتُطبق هذه الأنظمة في المواقع الأكثر حساسية كغرف التحكم في المفاعلات النووية ومراكز القيادة السرية ومخازن الأسلحة والمواد الكيميائية الخطرة."3"

ثانياً: أنظمة الإغلاق الأمني (الأقفال والحواجز الداخلية)

تُشـكل أنظمة الإغلاق والأقفال العنصـر المادي المكمل لأنظمة التحكم، حيث تحول دون فتح الأبواب أو الدخول إلى الغرف والمرافق دون الحصـــول على إذن نظام التحكم. وقد تطورت هذه الأنظمة بشـــكل كبير من الأقفال الميكانيكية التقليدية إلى الأقفال الإلكترونية والذكية، وتشـــمل الأقفال الميكانيكية عالية الأمان التي يصـــعب فتحها أو نســـخ مفاتيحها، والأقفال الإلكترونية التي تُفتح عبر بطاقات أو رموز، والأقفال الكهرومغناطيسـية التي تُسـتخدم في الأبواب الثقيلة وتُربط مباشـرة بأنظمة التحكم، والأقفال البيومترية التي لا تفتح إلا بعد مطابقة القياس الحيوي، وأنظمة الإغلاق المركزية التي تســـمح بالتحكم عن بعد بقفل وفتح مجموعة واســـعة من الأبواب من غرفة العمليات. وتُســـتخدم الحواجز الداخلية كبوابات دوارة (بوابات الرياح) التي تمنع عبور أكثر من شـــخص واحد في كل مرة، والبوابات الأمنية الداخلية الشـــبيهة بنقاط التفتيش الخارجية ولكن بعنصـــر المفاجأة الأقل، والأبواب المصـفحة المدرعة للمناطق ذات الحسـاسـية القصـوى، والأبواب المقاومة للحريق والانفجار في المنشآت النفطية والكيميائية."4"

ثالثاً: نظام إدارة الدخول المركزي(Access Control System)

يعمـل نظـام إدارة الـدخول المركزي بمثـابـة العقـل المـدبر لجميع عمليـات التحكم بالدخول في المنشـأة، حيث يُدير قاعدة بيانات الصـلاحيات لجميع الأفراد، ويُسـجل كافة عمليات الدخول والخروج بتفاصيلها الزمنية والمكانية، ويُصدر إنذارات فورية لأي محاولة دخول غير مصـرح بها، ويُتيح لوحات تحكم رسـومية تمكن المشـغلين

من رؤية حالة الأبواب في لحظة، ويُولد تقارير دورية عن أنماط الدخول لتحليلها وتحديد أي شذوذ. ويُعد هذا النظام قابلاً للتوسع والتكامل مع أنظمة أخرى كالمراقبة والإنذار، مما يجعله مركزاً لتجميع وتحليل المعلومات الأمنية. وتُدار صلاحيات النظام من خلال مستويات متعددة من المسؤولين، بحيث لا يمكن لأي فرد مهما كان موقعه تغيير الصلاحيات بشكل تعسفي، مما يضمن الرقابة المتبادلة ومنع التجاوزات."5"

رابعاً: إدارة صلاحيات الدخول وسياساتها

تُعد إدارة صلاحيات الدخول من المهام الأمنية الحساسة التي تستوجب دقة عالية وتحديثاً مستمراً، لضمان أن تتناسب صلاحيات كل فرد مع متطلبات وظيفته الحالية. وتشمل سياسات إدارة الصلاحيات وضع معايير واضحة لمنح الصلاحيات بناءً على الوصف الوظيفي وتقييم المخاطر، وتطبيق نظام المراجعة الدورية للصلاحيات بحيث تُلغى أو تُعدّل فور تغير مهام الفرد أو انتقاله أو انتهاء خدمته، وتطبيق مبدأ الفصل بين الصلاحيات بحيث لا يتمتع أي فرد بالقدرة على تنفيذ عملية حساسة بمفرده دون موافقة آخر، وتوثيق كل عملية منح أو تعديل أو إلغاء صلاحية مع ذكر المبررات والأطراف المعنية. وتُعد هذه السياسات وثائق حية تُراجع وتُحدث كلما طرأت تغيرات تنظيمية أو أمنية على المنشأة، وتُعمم على جميع المسؤولين عن إدارة الصلاحيات لضمان تطبيق موحد وعادل."6"

خامساً: التكامل مع أنظمة المراقبة والإنذار

تتحقق الفعالية القصوى لأنظمة الإغلاق والتحكم بالدخول عندما تُدمج مع أنظمة المراقبة والإنذار، إذ يُمكن عند محاولة دخول غير مصرح به أن تُوجه الكاميرات فوراً إلى موقع المحاولة وتسجيل المشهد، ويُطلق إنذار في غرفة العمليات ويُرسل تنبيه لرجال الأمن الموجودين في المكان، مع إمكانية إغلاق الأبواب المؤدية إلى المنطقة تلقائياً لعزل المخترق ومنعه من التقدم، وتسجيل وقت المحاولة وطبيعتها وهوية البطاقة أو القياس المستخدم في المحاولة للاستفادة منها في التحقيقات. ويُتيح هذا التكامل أيضاً إمكانية ربط نظام الدخول بجداول العمل ونظام الحضور

والانصراف، مما يساعد في التحقق من تواجد الموظفين في مواقعهم المقررة، وفي حالات الطوارئ يُمكن فتح جميع الأبواب تلقائياً لتسهيل الإخلاء مع الاحتفاظ بسجل لمن غادر ومن بقي."7"

سادساً: سياسات الطوارئ والإغلاق الشامل

تتطلب الظروف الاستثنائية تطبيق سياسات خاصة لإدارة الدخول، تختلف عن السياسات العادية وتستجيب لمتطلبات الأمن المشدد أو الإخلاء السريع. وتشمل هذه السياسات تفعيل نظام الإغلاق الشامل الذي يُقفل جميع الأبواب تلقائياً في حالات التهديد الأمني المباشر لعزل المنشأة ومنع الدخول أو الخروج، وتفعيل نظام الفتح الشامل الذي يُفتح جميع الأبواب تلقائياً في حالات الحريق أو الكوارث الطبيعية لتسهيل الإخلاء، وتفعيل نظام القفل المتدرج الذي يُغلق المناطق حسب الأولوية مع فتح ممرات الإخلاء، وتطبيق نظام الصلاحيات الاستثنائية الذي يمنح المسؤولين صلاحيات مؤقتة لتجاوز القيود في حالات الأزمات لإدارة العمليات الحرجة. وتُخطط لهذه السيناريوهات مسبقاً وتُدرَّب عليها الفرق الأمنية وطواقم الطوارئ، كما تُختبر أنظمة الإغلاق والفتح الشامل بشكل دوري للتأكد من عملها بكفاءة عند الحاجة."8"

سابعاً: التوثيق والتحليل الأمني لعمليات الدخول

يُشكل التوثيق الدقيق لعمليات الدخول والخروج أحد الأعمدة الأساسية لإدارة المنظومة الأمنية، إذ يُتيح تتبع حركة الأفراد داخل المنشأة وتحليلها لاكتشاف الأنماط غير الطبيعية. وتتضمن عملية التوثيق تسجيل هوية الداخل وتوقيت الدخول والخروج، والمنطقة التي دخل إليها، ووسيلة التحقق المستخدمة، وأي حوادث أو ملاحظات رافقت العملية، وحالة البوابة أو الباب في نهاية الدوام. وتُحلل هذه البيانات بشكل دوري للكشف عن السلوكيات المشبوهة كالدخول في أوقات غير معتادة، أو تكرار محاولات الدخول لمناطق غير مصرح بها، أو استخدام صلاحيات غير مناسبة، أو وجود فجوات زمنية غير مبررة، أو عدم تطابق بين سجلات الدخول ومهام الفرد المعلنة. ويُوصى بالاستعانة ببرمجيات تحليل البيانات الذكية

التي تستخدم تقنيات التعلم الآلي لكشف الأنماط الشاذة، مما يعزز القدرة على اكتشاف التهديدات الداخلية قبل أن تتطور إلى حوادث خطيرة."9"

ثامناً: الصيانة والاختبار الدوري للأنظمة

تخضع أنظمة الإغلاق والتحكم بالدخول كغيرها من الأنظمة التقنية لعوامل تآكل وأعطال محتملة، مما يستوجب برامج صيانة دورية واختبارات منتظمة لضمان استمرارية عملها بكفاءة. وتشمل هذه البرامج فحصاً دورياً للأقفال الإلكترونية والميكانيكية واختبار استجابتها، واختباراً لكافة أجهزة القراءة البيومترية والتأكد من دقتها، ومراجعة قواعد بيانات الصلاحيات والتأكد من تحديثها، واختباراً لأنظمة الطاقة الاحتياطية للبوابات والأبواب، وتقييماً دورياً لكفاءة نظام إدارة الدخول المركزي. ويُوصى بالاحتفاظ بسجلات مفصلة لأعمال الصيانة والأعطال التي تم إصلاحها، وتحليل هذه السجلات لتحديد الأنماط المتكررة ومعالجة أسبابها الجذرية، مع إجراء اختبارات مفاجئة وغير مجدولة لأنظمة الدخول للتأكد من جاهزية العاملين والأجهزة في جميع الأوقات."10"

وتُعد أنظمة الإغلاق والتحكم بالدخول من العناصر الأمنية الأكثر تفاعلاً مع التطور التكنولوجي، حيث تشهد تحديثات مستمرة في مجال القياسات الحيوية والتحقق عن بُعد وأنظمة التحليل الذكي. ويجب على المنشآت الحيوية مواكبة هذه التطورات واستثمارها في تعزيز منظومتها الأمنية، مع الأخذ في الاعتبار أن التكنولوجيا وحدها لا تكفي، بل لا بد من إدارتها بإجراءات بشرية وتنظيمية رصينة تضمن تحقيق الأهداف الأمنية بكفاءة وفعالية، وتجنب الاعتماد المفرط على الأنظمة الآلية دون مراجعة وتدقيق بشري، حيث يظل العنصر البشري هو صاحب القرار النهائي في العمليات الأمنية الحرجة."11"

وتُسهم هذه الأنظمة مجتمعة في تحقيق توازن دقيق بين متطلبات الأمن المشدد والمرونة التشغيلية اللازمة لاستمرارية العمل في المنشآت الحيوية، إذ تتيح حرية الحركة لمن لديهم الصلاحية مع منعها ممن ليسوا كذلك، وتوفر سجلاً دقيقاً يمكن الرجوع إليه عند التحقيق في الحوادث، كما تتيح للمسؤولين إمكانية تكييف مستويات

التأمين وفقاً لتطور التهديدات دون الحاجة إلى تغييرات جذرية في البنية التحتية "12".

وسائل الحماية من التهديدات الخارجية

تمثل التهديدات الخارجية أحد أخطر التحديات التي تواجه المنشـــآت الحيوية، نظراً لتنوع مصـادرها وتعاظم قدراتها التقنية والتسليحية في العقود الأخيرة. وتشـمل هذه التهديدات العمليات الإرهابية، والهجمات المسلحة، ومحاولات الاقتحام، والتخريب، والتجسس الصـناعي والسياسـي، والهجمات السيبرانية الموجهة من خارج المنشـأة، فضـلاً عن التهديدات الناجمة عن الكوارث الطبيعية أو الحوادث الصـناعية الكبرى. وتستند وسائل الحماية من هذه التهديدات إلى نهج متكامل يجمع بين العناصر المادية والتقنية والبشرية والإجرائية، ويعمل على مستويات متعددة تبدأ من الردع والكشف المبكر، مروراً بالمنع والتأخير، وصولاً إلى الاستجابة والتعافي."1"

أولاً: الحماية المحيطية من التهديدات الخارجية

تُعد الحمـايـة المحيطيـة خط الـدفـاع الأول والأكثر أهميـة في مواجهـة التهـديـدات الخارجية، حيث تهدف إلى منع أو تأخير وصـول أي تهديد إلى قلب المنشـأة. وتقوم هذه الحماية على عدة عناصـر متكاملة تبدأ بالأسـوار والحواجز المادية التي تشـكل حاجزاً ملموسـاً يصـعب اختراقه، وتشـمل الأسـوار الخرسـانية العالية والمدرعة للمنشـــآت عالية المخاطر، والأســـوار المعدنية المزودة بأنظمة كشـــف الاهتزاز والتوتر، والحواجز المانعة لاقتحام المركبات كالحواجز الخرســانية والأعمدة القابلة للرفع. وتأتي أنظمة الكشـــف المحيطية كعنصـــر ثانٍ يتمثل في أجهزة اســـتشـــعار الاهتزاز والحركة المثبتة على الأســـوار أو في التربة المحيطة، وكاميرات المراقبة الحرارية والنهارية التي تغطي كامل المحيط، وأجهزة الرادار الأرضـــي والليزر للكشـف عن أي تحرك غير عادي على مسـافات بعيدة، وأنظمة المسـح الإلكتروني للحرم التي تُنشـئ حقولاً كهرومغناطيسـية تُكسـر عند اختراقها. ويُعد نظام الإضـاءة المحيطية العنصر الثالث، حيث تضـيء كامل المسافة بين السور الخارجي والمباني الداخلية بشـكل متسـاوٍ، وتُسـتخدم أضـواء كاشـفة عالية الكثافة، وأضـواء مسـتشـعرة للحركة، وإضاءة طارئة تعمل عند انقطاع التيار الكهربائي."2"

ثانياً: الحماية المادية للمباني والمرافق الحيوية

إلى جانب الحماية المحيطية، تُستخدم وسائل حماية مادية للمباني والمرافق الحيوية ذاتها، لضمان عدم تمكن أي تهديدات خارجية تجاوزت المحيط من الوصول إلى الأصول الأكثر حساسية. وتشمل هذه الوسائل استخدام مواد بناء مقاومة للرصاص والانفجارات في الجدران الخارجية والنوافذ والأبواب، وتصميم المباني بمداخل ومخارج محدودة يسهل مراقبتها، واستخدام الزجاج المصفح والمقاوم للكسر في النوافذ والواجهات الزجاجية، وتزويد النوافذ والأبواب الخارجية بأنظمة قفل متطورة وأجهزة إنذار ضد الكسر، وإنشاء غرف آمنة داخل المباني يمكن اللجوء إليها في حالات الطوارئ. وتُستخدم في المنشآت عالية المخاطر أيضاً الجدران المزدوجة والفراغات الهوائية التي تحد من تأثير الانفجارات، والأبواب المدرعة المقاومة للرصاص والانفجار، وغرف التحصين الداخلية التي تُستخدم كملاجئ للعاملين في حالات الهجوم، بالإضافة إلى أنظمة تهوية وإطفاء حريق متطورة تمنع انتشار الحرائق أو الغازات السامة في حال وقوع هجوم كيميائي أو حريق."3"

ثالثاً: أنظمة الكشف المبكر عن التهديدات الخارجية

يُعد الكشف المبكر أحد أهم عناصر الحماية من التهديدات الخارجية، إذ يتيح فرصة ثمينة للاستجابة قبل أن يتحقق التهديد أو يتسبب في أضرار جسيمة. وتشمل أنظمة الكشف المبكر أجهزة استشعار الزلازل والاهتزازات للكشف عن محاولات الحفر تحت الأسوار أو الأنفاق، وأجهزة الكشف عن المتفجرات عن بُعد التي تعمل بتقنيات الأشعة السينية والرادار، وأنظمة كشف المواد الكيميائية والإشعاعية في الهواء والماء، وأجهزة استشعار الصوت والموجات فوق الصوتية لكشف تحركات أو أصوات غير معتادة، وأنظمة الرادار الثانوي والتصوير الفضائي للمنشآت الواسعة والمطارات، وأجهزة الكشف عن المركبات المشبوهة ككاميرات التعرف على لوحات الأرقام وتحليل سرعة الحركة. كما تشمل أنظمة الاستخبارات المفتوحة وتحليل وسائل التواصل الاجتماعي، التي تجمع وتحلل المعلومات المتداولة علناً للكشف عن أي تهديدات محتملة قبل وقوعها، بالتعاون مع الأجهزة الأمنية

والاستخباراتية المختصة التي تُزود المنشأة بالمعلومات الاستباقية عن التهديدات المحتملة."4"

رابعاً: الحماية من الهجمات السيبرانية الخارجية

تزايدت في السنوات الأخيرة الهجمات السيبرانية الموجهة ضد المنشآت الحيوية، وأصبحت تمثل أحد أخطر التهديدات الخارجية التي قد تؤدي إلى تعطيل عملياتها أو سرقة بياناتها الحساسة أو حتى تدمير أنظمتها التشغيلية. وتشمل وسائل الحماية من هذه الهجمات جدران الحماية الإلكترونية وأنظمة كشف التسلل ومنع الاختراق، التي تراقب حركة البيانات وتصد الهجمات المعروفة، وأنظمة التشفير القوي للبيانات أثناء التخزين والنقل، وأنظمة المصادقة متعددة العوامل للوصول إلى الأنظمة الحساسة، وفصل شبكات التحكم الصناعية عن شبكات الإنترنت العامة والشبكات الإدارية لمنع انتقال الاختراقات، وتحديث البرمجيات وأنظمة التشغيل باستمرار لسد الثغرات الأمنية، واستخدام أنظمة كشف التهديدات المتقدمة القائمة على الذكاء الاصطناعي وتحليل السلوك للكشف عن الهجمات غير المعروفة، وتنفيذ سياسات صارمة لإدارة صلاحيات الوصول الداخلي وتطبيق مبدأ "الحد الأدنى من الصلاحيات". وتشمل الحماية السيبرانية أيضاً تدريب العاملين على التصدي لهجمات التصيد والهندسة الاجتماعية، التي تُعد من أكثر وسائل الاختراق شيوعاً، فضلاً عن وضع خطط للاستجابة للحوادث السيبرانية لضمان التعافي السريع واستمرارية الأعمال."5"

خامساً: الحماية من الهجمات بالمركبات المفخخة

تمثل الهجمات بالمركبات المفخخة أحد أخطر التهديدات الخارجية التي تواجه المنشآت الحيوية، نظراً لقدرتها على التسبب في خسائر بشرية ومادية هائلة. وتشمل وسائل الحماية من هذا النوع من التهديدات إنشاء مسافات أمان كافية بين الطرق العامة ومباني المنشأة، تُعرف بالمناطق العازلة، تمنع وصول المركبات المفخخة إلى أهدافها الحيوية، وتصل هذه المسافات في المنشآت عالية المخاطر إلى مئات الأمتار. وتُستخدم الحواجز المادية المانعة للاختراق كالحواجز الخرسانية المرتفعة

والأعمدة القابلة للرفع والأنظمة الشبكية الممتدة حول المحيط، التي تُوضع بشكل يمنع المركبات من الاقتراب أو اختراق الحرم بسرعة عالية. وتُشغل كاميرات التعرف على لوحات الأرقام في المداخل لتسجيل المركبات الداخلة والخارجة ومقارنتها بقواعد البيانات المطلوبة أمنياً، وتُستخدم أنظمة الكشف عن المتفجرات للمركبات عند نقاط التفتيش، وأجهزة المسح الأرضي للكشف عن أي تغيرات في هيكل المركبة أو إضافات غير معتادة. ويُمنع وقوف المركبات في المناطق القريبة من المباني الحيوية أو تحت النوافذ، وتُخصص مواقف بعيدة ومحصنة، خاصة للزوار والمقاولين. كما تُطبق سياسات صارمة لدخول الشاحنات والخزانات التي تُعد أهدافاً محتملة لحمل كميات كبيرة من المتفجرات، وتُخضع لتفتيش دقيق عند نقاط الدخول."6"

سادساً: الحماية من الهجمات الجوية والطائرات المسيَّرة

مع تزايد استخدام الطائرات المسيَّرة بدون طيار (الدرون) في العمليات الاستطلاعية والهجومية، أصبحت تشكل تهديداً خارجياً متنامياً للمنشآت الحيوية. وتشمل وسائل الحماية من هذا النوع من التهديدات تركيب أنظمة كشف الطائرات المسيَّرة باستخدام الرادار وتقنيات الترددات الراديوية والاستشعار الصوتي والبصري، التي ترصد وتتعقب الطائرات المسيَّرة في محيط المنشأة، واستخدام أنظمة التشويش الإلكتروني التي تشوش على ترددات التحكم وإشارات الـ (GPS)لمنع الطائرة من الوصول إلى هدفها أو إعادتها إلى نقطة انطلاقها، وتوظيف أنظمة الصيد الشبكية أو الطائرات المعترضة التي تتعامل مع الطائرات المسيَّرة المعادية في الجو، وتطبيق أنظمة الحماية المادية كتغطية المنشآت الحساسة بشبكات مقاومة للاختراق من الأعلى. كما تُسن سياسات تنظيمية تُحدد مناطق الطيران المحظورة حول المنشآت الحيوية، وتُفعّل آليات التنسيق مع سلطات الطيران المدني والأمنية لإبلاغها بأي اختراقات جوية، وتُدرَّب الفرق الأمنية على التعامل مع مثل هذه الحوادث، خاصة تلك التي قد تحمل مواد متفجرة أو كيماوية خطيرة."7"

سابعاً: الحماية من التهديدات الكيميائية والبيولوجية والإشعاعية

تواجه بعض المنشآت الحيوية، كالمصانع الكيميائية والمفاعلات النووية والمختبرات البيولوجية، تهديدات خارجية تتمثل في هجمات قد تسفر عن تسرب مواد خطيرة. وتشمل وسائل الحماية من هذه التهديدات أنظمة الكشف المبكر للغازات والمواد الكيميائية والإشعاعية المنتشرة في الهواء والماء حول المنشأة، ووحدات الترشيح والتنقية في أنظمة التهوية لمنع دخول الغازات السامة إلى المباني، وتوفير ملاجئ محكمة الإغلاق ومزودة بأنظمة تنقية هواء مستقلة يمكن للعاملين الاحتماء بها، وتطبيق إجراءات العزل السريع للمناطق الملوثة ومنع انتشار المواد الخطرة، ووضع خطط إخلاء متخصصة للتعامل مع حالات التسرب الكيميائي أو الإشعاعي، وتجهيز فرق الاستجابة بمعدات الحماية الشخصية المتخصصة كالأقنعة والبدلات الواقية. وتشمل الحماية أيضاً التعاون مع الهيئات البيئية والصحية والدفاع المدني لتقييم الأثر وتنفيذ خطط التطهير والمعالجة، وتطوير أنظمة الإنذار الموجهة للعاملين والسكان المحيطين لتحذيرهم من أي تسرب خطير."8"

ثامناً: التعاون مع الأجهزة الأمنية والاستخباراتية

لا يمكن للمنشآت الحيوية مواجهة التهديدات الخارجية بمفردها دون تعاون وثيق مع الأجهزة الأمنية والاستخباراتية الوطنية والدولية. ويشمل هذا التعاون تبادل المعلومات الاستخبارية والتحذيرية حول التهديدات المحتملة، والمشاركة في تمارين وخطط الطوارئ الوطنية، والاستفادة من الخبرات الفنية والتقنية للجهات الحكومية في تطوير أنظمة الحماية، والحصول على الدعم الأمني المباشر عند الحاجة كتوفير حراسات إضافية أو غطاء جوي. وتُعقد اجتماعات دورية بين مسؤولي الأمن في المنشأة والجهات الأمنية لمراجعة مستويات التهديد وتحديث الإجراءات، كما تُسهم هذه العلاقات في تسهيل إجراءات التراخيص والتصاريح الأمنية للموظفين والمقاولين، وضمان الاستجابة السريعة في حالات الطوارئ التي تتجاوز قدرات المنشأة الذاتية. ويُعد بناء الثقة والعلاقات المهنية مع هذه الأجهزة استثماراً طويل الأمد يعزز مناعة المنشأة ضد مختلف التهديدات."9"

تاسعاً: التخطيط للاستمرارية والتعافي بعد التهديدات الخارجية

تكتمل منظومة الحماية من التهديدات الخارجية بوضع خطط للاستمرارية والتعافي تضمن عودة المنشأة إلى العمل بأسرع وقت ممكن بعد تعرضها لأي هجوم أو حادث. وتشمل هذه الخطط تحديد الوظائف الحيوية التي يجب أن تستمر في العمل بأي ثمن، وتوفير أنظمة بديلة واحتياطية للمعدات والبرمجيات الأساسية، وإعداد قواعد بيانات احتياطية مؤمنة خارج الموقع، وتحديد الموردين البديلين للمواد والمعدات، وتدريب فرق متخصصة في التعافي من الكوارث، ووضع جدول زمني واضح لإعادة التشغيل بعد الحوادث. وتُجرى تدريبات واختبارات دورية لخطط الاستمرارية، لتقييم فعاليتها واكتشاف الثغرات فيها ومعالجتها قبل وقوع الطوارئ الحقيقية، مما يضمن أن المنشأة لا تتوقف عن العمل إلا لأقصر فترة ممكنة حتى في أصعب الظروف."10"

وتُعد وسائل الحماية من التهديدات الخارجية نظاماً ديناميكياً يتطور باستمرار لمواكبة تطور التهديدات نفسها، حيث تتبادل العناصر المادية والتقنية والبشرية الأدوار في منظومة دفاعية متكاملة، وتظل مراجعة هذه الوسائل وتطويرها مسؤولية مستمرة تقع على عاتق إدارة الأمن في المنشأة، بالتعاون مع الخبراء والجهات المعنية، لضمان بقاء المنشأة في منأى عن المخاطر الخارجية المتنامية والمتجددة "١١". وفي هذا السياق، تبرز الحاجة إلى ثقافة أمنية راسخة لدى جميع العاملين، تمكنهم من التعرف على مؤشرات التهديدات والإبلاغ عنها، وتجعل منهم عيوناً وآذاناً أمنية تسهم في حماية المنشأة من مختلف الأخطار الخارجية."12"

تأمين مواقع البنية التحتية الحيوية

تمثل البنية التحتية الحيوية العمود الفقري للدولة الحديثة، وتشمل منظومات متشابكة ومعقدة من المرافق والشبكات التي تؤمن استمرارية الخدمات الأساسية كالمياه والطاقة والاتصالات والنقل والصحة. وتتسم هذه المواقع بطابعها الاستراتيجي وانتشارها الجغرافي الواسع، وتنوع أنشطتها التشغيلية، وكثرة نقاط التعرض فيها للتهديدات، مما يجعل تأمينها مهمة بالغة التعقيد تتطلب نهجاً شاملاً ومتكاملاً يجمع بين الحماية المادية والتقنية والإجرائية والبشرية، مع مراعاة خصوصية كل قطاع وطبيعة موقعه الجغرافي وحجم التهديدات الموجهة إليه."1"

أولاً: تصنيف البنية التحتية الحيوية وتحديد أولويات الحماية

لا يمكن تأمين جميع عناصر البنية التحتية الحيوية بالمستوى نفسه من الحماية، نظراً لتفاوت درجة خطورتها وأهميتها وتأثير تعطلها. ولذا، يُعد تصنيف هذه المواقع وتحديد أولويات الحماية من الخطوات التأسيسية لأي استراتيجية أمنية. ويتم التصنيف وفق معايير متعددة كالأهمية الوطنية للمنشأة في ضمان استمرار الخدمات الأساسية، والتأثير المحتمل لتعطلها على الاقتصاد والصحة العامة والأمن الوطني، ومدى قابليتها للتعرض للتهديدات الطبيعية والبشرية، وكثافة الحركة والاعتماد عليها من قبل قطاعات أخرى. ويُقسّم التصنيف الأمني للمنشآت عادة إلى فئات متدرجة كالفئة الأولى (ذات الأهمية القصوى)، والفئة الثانية (ذات الأهمية الكبرى)، والفئة الثالثة (ذات الأهمية المتوسطة). وتُخصص لكل فئة مستويات حماية تتناسب مع تصنيفها، وتُحدد الموارد المادية والبشرية والتقنية المطلوبة، فضلاً عن وتيرة التدريبات والمراجعات الأمنية. وتُستخدم أدوات كتحليل نقاط الضعف وتقييم المخاطر لتحديد الأولويات، مع مراعاة تحديث هذا التصنيف بشكل دوري لمواكبة التطورات في طبيعة التهديدات أو التوسع في الشبكات والمرافق."2"

ثانياً: تأمين شبكات الطاقة والكهرباء

تُعد شبكات الطاقة والكهرباء من أكثر عناصر البنية التحتية حساسية وأعلاها تعرضاً للتهديدات، حيث يؤدي تعطلها إلى شل جميع القطاعات الأخرى. وتشمل

وسـائل تأمينها حماية محطات التوليد والشـبكات الناقلة ومحطات التوزيع، وذلك من خلال أســوار وحواجز مادية عالية، وأنظمة مراقبة محيطية متطورة، ونقاط تفتيش مشـددة للموظفين والمركبات، وأنظمة كشـف تسـرب وانقطاع في الخطوط الناقلة. وتُولى عناية خاصـــة بحماية أنظمة التحكم والتشـــغيل (SCADA) من الهجمات السـيبرانية، من خلال فصـل هذه الأنظمة عن الشـبكات المفتوحة واسـتخدام أنظمة تشـفير قوية ومصـادقة متعددة العوامل، مع تركيب أنظمة مراقبة للشـبكة لكشـف أي أنشطة غير طبيعية. كما تُستخدم أنظمة الكشف عن الطائرات المسيرة حول محطات التوليد والمحولات الرئيسية، وتُجهز بخطط طوارئ سريعة لإعادة التشغيل في حال انقطاع التيار، وتُقام شـراكات مع مشـغلي الشـبكات المجاورة لتوفير تغذية احتياطية في حـالات الطوارئ. ويُوصـــى بإجراء تدريبات دورية لمحاكاة ســـيناريوهات الهجمات الإلكترونية والفيزيائية على شبكات الطاقة، لضمان جاهزية الفرق للتعامل مع مختلف الاحتمالات."3"

ثالثاً: تأمين شبكات المياه والصرف الصحي

تمثل شـبكات المياه والصـرف الصـحي عنصـراً حيوياً لا غنى عنه، إذ يرتبط تلوثها أو انقطاعها مباشرة بالصحة العامة والسلامة البيئية. وتشمل إجراءات تأمينها حماية مصـادر المياه كالسـدود والآبار ومحطات التحلية بمسـتويات أمنية مشـددة، ومراقبة نوعية المياه بشـكل مسـتمر للكشـف عن أي ملوثات كيميائية أو بيولوجية، وتركيب أنظمة كشـف التسـلل والتلوث على امتداد خطوط النقل الرئيسـية، وتأمين محطات الضـــخ والمعالجة بأنظمة مراقبة وتحكم تمنع العبث أو التخريب. وتشـــمل الحماية أيضاً تأمين الخزانات الاستراتيجية ومحطات التوزيع ضد التلوث المتعمد، واستخدام أنظمة تحذير مبكر لاكتشاف أي تغيرات في ضغط المياه أو جودتها، وتدريب الفرق على الاســتجابة الســريعة لحالات التلوث أو الانقطاع مع توفير خطط بديلة للإمداد كالصـهاريج أو الآبار الاحتياطية. وتُعد حماية الأنظمة الإلكترونية للتحكم في شبكات المياه من الاختراقات الســـيبرانية أولوية متزايدة، إذ يمكن أن تؤدي الهجمات على

هذه الأنظمة إلى تعطيل التوزيع أو تغيير نســـب المعالجة الكيميائية بطرق خطيرة "4".

رابعاً: تأمين شبكات الاتصالات وتقنية المعلومات

تشــكل شــبكات الاتصـــالات وتقنية المعلومات الشــريان العصــبي الذي يربط كافة قطـاعات البنيـة التحتيـة، ويعد تعطلها أو اختراقها شـــللاً لكـافة الأنظمـة الأخرى. وتشـمل وســائل تأمينها حماية مراكز البيانات الرئيســية والموزعة بأســوار وأنظمة مراقبة مشـــددة، وتأمين الكابلات البحرية والبرية الرئيســية بمناطق عازلة وأنظمة إنذار وكشــف للقطع أو العبث، واســتخدام أنظمة التشــفير القوي والتبديل المســار للاتصــالات الحســاسـة، وتطبيق أنظمة كشـف التسـلل ومنع الاختراق في الشـبكات، وتأمين نقاط التبادل الرئيســـية (الإنترنت - البوابات) بأعلى مســـتويات الحماية. ويُوصــى بإنشــاء شـبكات اتصــال بديلة مستقلة عن الشـبكة الرئيسـية لاستخدامها في حـالات الطوارئ، وتوفير مصـــــادر طـاقـة احتيـاطيـة لمراكز البيـانـات والمحطـات الأســاســية لضــمان اســتمراريتها عند انقطاع الكهرباء، والاحتفاظ بنســخ احتياطية محدثة من البيانات الحســـاســـة في مواقع جغرافية متباعدة، مع إجراء اختبارات اختراق دورية لشــبكات الاتصـــالات لكشــف الثغرات ومعالجتها قبل أن يســتغلها المهاجمون. كما تُعد حماية البنية التحتية للاتصـــالات من الهجمات الإلكترونية المتقدمة (APT) أولوية قصوى، وتستلزم استخدام أنظمة كشف متقدمة تعتمد على الذكاء الاصطناعي وتحليل السلوك."5"

خامساً: تأمين المطارات والموانئ والمنافذ الحدودية

تمثل المطارات والموانئ نقاط دخول وخروج حيوية تربط الدولة بالعالم الخارجي، وتتطلب مســتويات عالية من التأمين نظراً لكثافة الحركة وتنوع التهديدات المحتملة. وتشمل إجراءات تأمينها أنظمة تفتيش متطورة للأفراد والبضـائع والأمتعة باستخدام أجهزة الأشـعة السـينية وكشـف المتفجرات والمواد المشـعة، وتطبيق أنظمة التعرف على الوجه والقياســـات الحيوية للركاب والعاملين، وتأمين الممرات المائية والجوية المحيطة بأنظمة رادار وكشـف ومنع اقتحام، وحماية البضـائع الخطرة والمشـحونات

الاستراتيجية بإجراءات أمنية مشددة. وتُستخدم أنظمة مراقبة محيطية شاملة تغطي كامل حدود الميناء أو المطار، مع مناطق عازلة ومسافات أمان لمنع وصول المركبات المفخخة، وتُطبق بروتوكولات تعاون أمني مع سلطات الطيران المدني والملاحة البحرية والأجهزة الأمنية، وتُجرى تدريبات دورية مشتركة لمحاكاة سيناريوهات الإرهاب والهجمات الإلكترونية والكوارث الطبيعية. وتُعد حماية أنظمة المراقبة الجوية والبحرية والأنظمة الإلكترونية للملاحة من الهجمات السيبرانية أمراً حيوياً، إذ يمكن أن تؤدي إلى حوادث كارثية في حال اختراقها."6"

سادساً: تأمين المستشفيات والمرافق الصحية الحيوية

تُعد المستشفيات والمرافق الصحية الحيوية من المنشآت ذات الأولوية القصوى في أي خطة أمنية، إذ يرتبط تعطلها أو تعرضها للاختراق بحياة المرضى وسلامتهم. وتشمل إجراءات تأمينها حماية أقسام الطوارئ والعمليات والعناية المركزة ومخازن الأدوية والمختبرات بإجراءات دخول صارمة وأنظمة مراقبة، وتأمين أنظمة المعلومات الصحية وسجلات المرضى من الاختراقات والهجمات الإلكترونية التي قد تؤدي إلى تعطيل الخدمات أو سرقة البيانات، وضمان استمرارية الخدمات الحيوية كالأكسجين والكهرباء والماء عبر مولدات احتياطية وخزانات بديلة، وتوفير ممرات آمنة للإخلاء الطبي ونقل المصابين. وتشمل الحماية أيضاً تأمين سلسلة التوريد الطبية لضمان وصول الأدوية والمستلزمات الحيوية دون انقطاع أو تلاعب، وتدريب الكوادر الطبية والإدارية على إجراءات الأمن والسلامة والتصرف في حالات الطوارئ، مع إجراء تدريبات دورية لمحاكاة سيناريوهات الأزمات كالهجمات الإرهابية أو الكوارث الجماعية أو تفشي الأوبئة. وتُعد حماية المستشفيات من الهجمات السيبرانية أولوية متزايدة، خاصة مع تزايد استخدام الأجهزة الطبية المتصلة بالشبكات وأنظمة السجلات الإلكترونية."7"

سابعاً: تأمين المنشآت النووية والإشعاعية

تمثل المنشآت النووية والإشعاعية أخطر عناصر البنية التحتية الحيوية من حيث العواقب المحتملة لأي حادث أمني، إذ قد يتسبب أي خرق فيها بكارثة بيئية وإنسانية

تمتد آثارها عبر الحدود. وتشمل إجراءات تأمينها أعلى مستويات الحماية المحيطية من أسوار وحواجز مضادة للرصاص والانفجارات، وأنظمة كشف محيطية متطورة متعددة الطبقات، ونقاط تفتيش مشددة للغاية مع تحقق بيومتري صارم، وأنظمة كشف إشعاعي دائمة في المحيط والمداخل، وحماية أنظمة التشغيل والتحكم بأعلى معايير الأمن السيبراني وعزلها تماماً عن أي شبكة خارجية، وتطبيق سياسات صارمة للتحقق من الخلفيات الأمنية للعاملين وتقييد صلاحياتهم بأقصى درجة. وتُوضع خطط طوارئ مفصلة للتعامل مع أي تسرب إشعاعي أو هجوم إرهابي، وتُجرى تدريبات مشتركة مع الجهات الوطنية والدولية، وتُلتزم المنشآت النووية بمعايير وإجراءات الوكالة الدولية للطاقة الذرية (IAEA) باستمرار، وتُخضع لتفتيش ومراجعة دورية من مفتشين دوليين للتأكد من التزامها بأعلى مستويات الأمن والسلامة. وتُعد حماية المواد النووية من السرقة أو الاستيلاء غير المشروع أولوية أمنية كبرى، نظراً لاحتمال استخدامها في صنع أسلحة إشعاعية أو نووية بدائية."8"

ثامناً: تأمين شبكات النقل والمواصلات

تشمل شبكات النقل الطرق والسكك الحديدية والجسور والأنفاق، وتعتمد عليها حركة الأفراد والبضائع والخدمات، مما يجعل تعطيلها أو استهدافها مؤثراً مباشراً على الاقتصاد والحياة اليومية. وتشمل إجراءات تأمينها حماية النقاط الحيوية كالجسور الكبرى والأنفاق ومحطات القطارات الرئيسية بأنظمة مراقبة ومنع دخول، وتركيب كاميرات مراقبة على طول الطرق السريعة والخطوط الحديدية لكشف الأنشطة المشبوهة، وتأمين أنظمة التحكم في حركة القطارات والطائرات من الهجمات السيبرانية، ووضع خطط لتحويل حركة المرور في حالات الطوارئ أو تعطل الشبكات. وتشمل الحماية أيضاً تدريب الكوادر على التعامل مع حوادث النقل الكبرى كاصطدام القطارات أو انهيار الجسور أو تسرب مواد خطرة أثناء النقل، والتنسيق مع الدفاع المدني والإسعاف لتجهيز فرق استجابة سريعة على طول خطوط النقل الرئيسية. وتُعد حماية البنية التحتية للنقل من التخريب والإرهاب من

الأولويات الأمنية، خاصـــة في النقاط التي تشـــهد ازدحاماً أو تقاطعات حيوية، وتُســـتخدم أنظمة كشـــف المتفجرات في محطات القطارات والمترو، مع تطبيق إجراءات تفتيش عشوائية للركاب والأمتعة."9"

تاسعاً: التنسيق المشترك بين قطاعات البنية التحتية

لا يمكن تأمين البنية التحتية الحيوية بمعزل عن بعضـــها البعض، بل يتطلب الأمر تنسيقاً وثيقاً ومستمراً بين جميع القطاعات المعنية، لتشكيل منظومة دفاعية متكاملة تتبادل المعلومات والتجارب والموارد. وتشـمل آليات التنسـيق إنشـاء مركز وطني لأمن البنية التحتية يجمع ممثلين عن جميع القطاعات الحيوية، وتشـــكيل فرق عمل مشـتركة لدراسـة التهديدات المشـتركة ووضـع اسـتراتيجيات موحدة لمواجهتها، وتوحيد معـايير وإجراءات الأمن بين القطـاعـات المختلفـة، وتبـادل المعلومـات الاستخبارية حول التهديدات المحتملة بشكل فوري وآمن، وتنظيم تدريبات ومحاكاة مشـــتركة تجمع فرقاً من قطاعات متعددة لاختبار الاســـتجابة للأزمات المعقدة والممتدة. ويُوصـى بوضع بروتوكولات للاتصـال الطارئ بين القطاعات، واتفاقيات لدعم الموارد في حالات الأزمات الكبرى، وخطط مشتركة للاستمرارية تضمن عدم توقف قطاع بسبب تعطل قطاع آخر، مع إشراك القطاع الخاص في هذه التنسيقات نظراً لامتلاكه جزءاً كبيراً من البنية التحتية الحيوية في كثير من الدول."10"

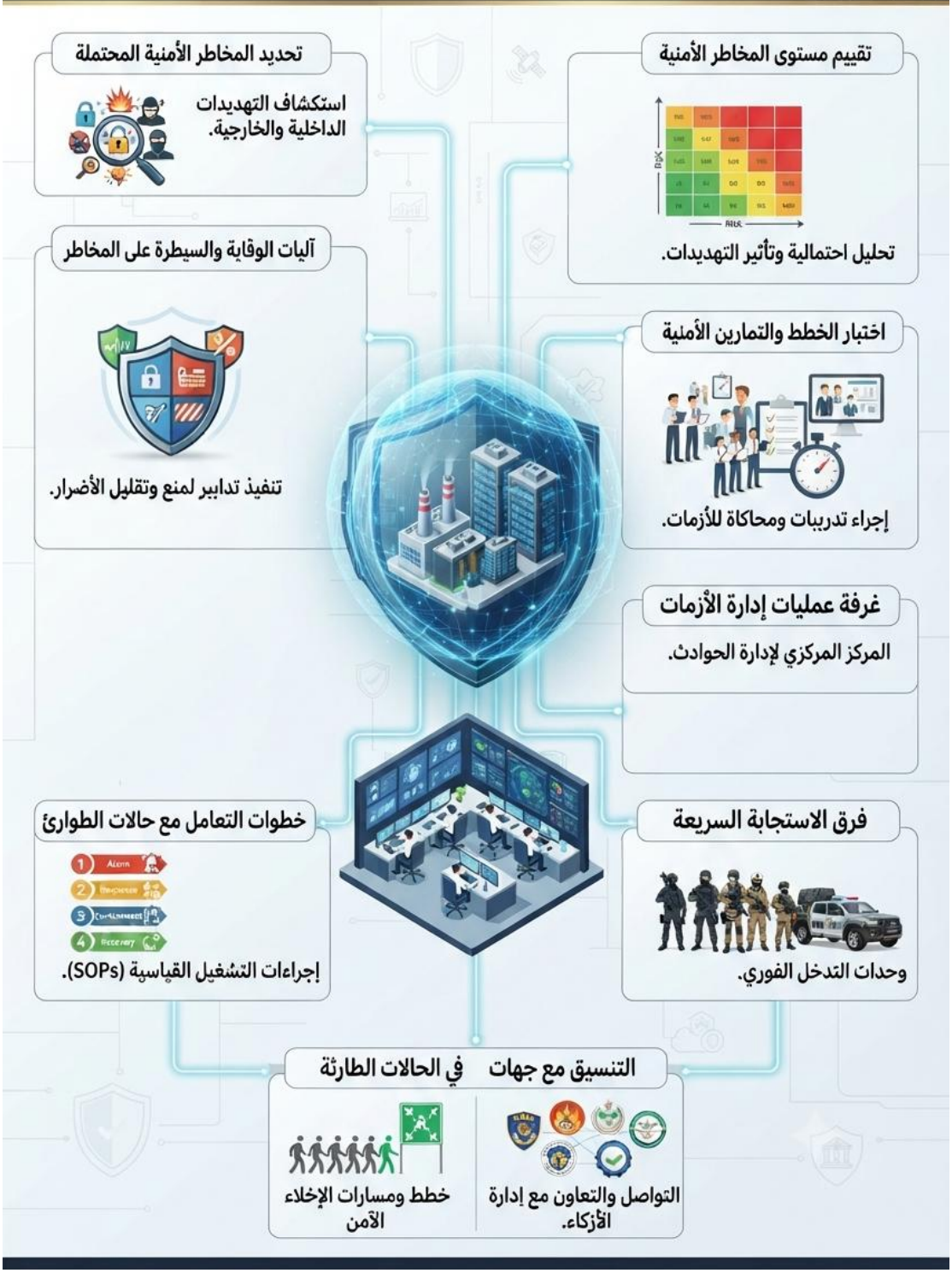
عاشراً: المراجعة والتطوير المستمر لأمن البنية التحتية

تظل التهديدات الموجهة للبنية التحتية الحيوية في تطور مســـتمر، مما يســـتوجب مراجعة وتطويراً دائماً لإجراءات وأنظمة الأمن المعمول بها، لمواكبة التغيرات في طبيعة وطرق الهجمات والوسـائل التقنية المسـتخدمة فيها. وتشـمل المراجعة تقييماً دورياً شاملاً للثغرات الأمنية ونقاط الضعف في كل منشأة، وتحليلاً مستمراً لبيانات الحوادث الأمنية السـابقة واسـتخلاص الدروس منها، ومتابعة التطورات التكنولوجية وتقييم إمكانية تطبيقها في تحسـين الأمن، وتحديث السـياسـات والإجراءات الأمنية وفقاً للمتغيرات، وإعادة تصـــنيف الأولويات الأمنية بناءً على تغيرات مســـتويات التهديد. ويُوصـــى بإجراء مراجعات أمنية مســـتقلة بواســـطة خبراء خارجيين

متخصـصـين، واسـتخدام مؤشـرات أداء أمني قابلة للقياس لتقييم فعالية الإجراءات وتحديد مجالات التحسين، مع الأخذ في الاعتبار أن أمن البنية التحتية ليس مشروعاً له نقطة نهاية، بل هو عملية مستمرة تتطلب التزاماً دائماً وجهوداً متواصلة من كافة المعنيين على المستويات الوطنية والمحلية والمؤسسية."11"

وتُمثل حماية البنية التحتية الحيوية اسـتثماراً اسـتراتيجياً في اسـتقرار الدولة وأمنها القومي، ويجب أن تنظر إليها الحكومات والمؤسـسـات كأولوية تتجاوز التكاليف المباشـرة، وأن تخصـص لها الموارد المالية والبشـرية والتقنية الكافية، مع إدراك أن تكلفة الإهمال الأمني تفوق بكثير تكلفة الوقاية والاسـتعداد، وأن أي ثغرة في أي موقع من هذه المواقع قد تكون نقطة انطلاق لانهيار متسلسل يؤثر في كامل منظومة الخدمات الوطنية."12"

الوحدة الثالثة:
إدارة المخاطر الأمنية



الوحدة الثالثة: إدارة المخاطر الأمنية

تمثل إدارة المخاطر الأمنية الركيزة المنهجية التي تقوم عليها كافة عمليات التخطيط والتنفيذ والتقييم في مجال أمن المنشـــآت الحيوية، إذ توفر الإطار العلمي والمنطقي لتحديد الأولويات وتخصيص الموارد واتخاذ القرارات الأمنية الرشيدة. وتقوم فلسفة إدارة المخـاطر على مبدأ أن الأمن المطلق غير قـابل للتحقيق، وأن الهدف الأكثر واقعية هو الوصـــول إلى مســـتوى مقبول من المخاطر يتوافق مع طبيعة المنشـــأة وأهميتها وقدراتها وإمكانياتها، مع إبقاء هذه المخاطر تحت الســـيطرة والمراقبة المستمرة. وتتضمن إدارة المخاطر الأمنية سلسلة من العمليات المنهجية المترابطة، تبدأ بتحديد الأصـول التي تسـتوجب الحماية، وتمر بتقييم التهديدات ونقاط الضـعف، وتحليل المخاطر وتقدير درجتها، ثم وضـــع وتنفيذ اســـتراتيجيات للتعامل معها، وانتهاء بالمراقبة والمراجعة المسـتمرة لضـمان فاعلية الإجراءات المتخذة وتحديثها باستمرار."1"

أولاً: تحديد الأصول وتصنيفها

تُعد عملية تحديد الأصـول وتصـنيفها الخطوة الأولى والأكثر جوهرية في أي عملية إدارة مخاطر أمنية، إذ لا يمكن حماية ما لا يُعرف أو يُقدّر. وتشـــمل الأصـــول في ســياق المنشـــآت الحيوية الأصـــول المادية (كالمباني والمنشـــآت والمعدات والآلات والمخزون الاســـتراتيجي)، والأصـــول البشـــرية (كالكوادر العاملة في المناصـــب الحيوية والخبرات النادرة)، والأصـــول المعلوماتية (كالبيانات والوثائق الحســـاســـة والملكية الفكرية والســـجلات التشـــغيلية)، والأصـــول الســـماتية (كســـمعة المنشـــأة وصـــورتها العامة والثقة المكتســـبة من العملاء والشـــركاء)، والأصـــول التشـــغيلية (كالأنظمة والإجراءات والعمليات التي تضـــمن اســـتمرارية العمل). ويُصـــنف كل أصـــل وفق معايير محددة تشـــمل القيمة الاقتصـــادية للأصـــل وتكلفة اســـتبداله أو إصلاحه، والأهمية الاستراتيجية في استمرار عمل المنشأة، ومدى حساسية الأصل وتأثير فقده أو تعطله، وإمكانية اســـتبداله أو تعويضـــه، ومدى تعرضـــه للتهديدات

المختلفة. ويُستخدم نظام التصنيف لترتيب الأولويات في الحماية، بحيث تُخصص أعلى مستويات الحماية للأصول الأكثر قيمة وأهمية، مع مراعاة تحديث التصنيف بشكل دوري كلما طرأت تغيرات على طبيعة المنشأة أو نشاطها أو أصولها، أو عند اكتشاف أصول جديدة أو تغير في قيمة أو أهمية الأصول القائمة."2"

ثانياً: تحديد التهديدات وتقييمها

يُعد تحديد التهديدات المحتملة وتقييمها الخطوة الثانية في عملية إدارة المخاطر، وتهدف إلى فهم طبيعة الأخطار التي قد تواجه المنشأة ومصادرها واحتمالية وقوعها وحجم تأثيرها المحتمل. وتُصنف التهديدات عادةً إلى تهديدات طبيعية (كالزلازل والفيضانات والأعاصير والعواصف والحرائق الطبيعية)، وتهديدات بشرية متعمدة (كالإرهاب والتخريب والهجمات السيبرانية والتجسس والسرقة والاقتحام)، وتهديدات بشرية غير متعمدة (كالأخطاء البشرية والإهمال وسوء التدريب)، وتهديدات تكنولوجية (كالأعطال التقنية وانهيار الأنظمة واختراقات الشبكات)، وتهديدات بيئية (كالتلوث والتغيرات المناخية والأوبئة). ويُستخدم في تقييم التهديدات عدة أدوات ومنهجيات، منها تحليل السيناريوهات الذي يرسم سيناريوهات مختلفة للتهديدات المحتملة وكيفية تطورها، وتحليل الاتجاهات الذي يدرس أنماط التهديدات السابقة ويتنبأ بالمستقبلية منها، وتقييم المصادر الذي يحلل قدرات ونوايا الجهات المهددة، والاستخبارات الأمنية المفتوحة التي تجمع المعلومات من المصادر المتاحة علناً. ويُعبّر عن التهديد عادةً بمتغيرين أساسيين: الاحتمالية (وهي مدى احتمال وقوع التهديد خلال فترة زمنية معينة)، والتأثير (وهو حجم الضرر المتوقع في حال وقوع التهديد). ويُستخدم هذا التقييم لتصنيف التهديدات من شديدة إلى منخفضة، وتوجيه الجهود والموارد نحو التهديدات الأعلى خطراً."3"

ثالثاً: تحليل نقاط الضعف

نقاط الضعف هي الثغرات أو القصور في أنظمة وإجراءات وعناصر المنشأة التي يمكن أن يستغلها التهديد لإلحاق الضرر بالأصول. ويُعد تحليل نقاط الضعف وتقييمها الخطوة الثالثة في إدارة المخاطر، ويهدف إلى التعرف على مواطن

القصور في الحماية وتحديد أولويات معالجتها. وتشمل نقاط الضعف المحتملة نقاط ضعف في التصميم الهندسي للمنشأة (كوجود مداخل غير محمية، أو نوافذ سهلة الكسر، أو أسوار منخفضة)، ونقاط ضعف في الأنظمة التقنية (كثغرات في أنظمة التحكم بالدخول، أو برمجيات قديمة غير محدثة، أو شبكات غير مشفرة)، ونقاط ضعف بشرية (كنقص التدريب الأمني للعاملين، أو ضعف الوعي الأمني، أو إهمال الإجراءات)، ونقاط ضعف إجرائية (كغياب سياسات مكتوبة، أو عدم وضوح الصلاحيات والمسؤوليات، أو غياب خطط الطوارئ)، ونقاط ضعف تنظيمية (كضعف التنسيق بين الإدارات، أو غياب آليات الإبلاغ، أو عدم كفاية الموارد المالية المخصصة للأمن)، ونقاط ضعف في سلسلة التوريد (كاعتماد المنشأة على موردين غير مؤمنين، أو وجود ثغرات في أمن نقل المواد والمعدات). ويُستخدم في تحليل نقاط الضعف أدوات متنوعة كعمليات التفتيش الأمني والتدقيق، والاختبارات العملية للأنظمة، وتحليل الحوادث السابقة، ومقارنة الأداء بالمعايير والممارسات الفضلى، واستشارة الخبراء الخارجيين. وتُحدد نقاط الضعف وفق معايير مثل سهولة الاستغلال (مدى سهولة قيام التهديد باستغلال هذه الثغرة)، وتأثير الاستغلال (حجم الضرر الناتج عن استغلال الثغرة)، واكتشاف الثغرة (مدى سهولة اكتشاف وجود الثغرة من قبل المهاجمين أو المختصين). ويُستخدم هذا التحليل لتوجيه جهود المعالجة نحو نقاط الضعف الأكثر خطورة والتي يسهل استغلالها."4"

رابعاً: تحليل المخاطر وتقديرها

يُمثل تحليل المخاطر وتقديرها القلب المنهجي لعملية إدارة المخاطر، إذ يجمع بين مخرجات خطوات تحديد الأصول والتهديدات ونقاط الضعف لتوليد صورة متكاملة عن المخاطر التي تواجه المنشأة. ويُعرّف الخطر عادةً بأنه دالة تجمع بين احتمال وقوع التهديد وحجم تأثيره، مع مراعاة نقاط الضعف الموجودة التي قد تزيد من الاحتمالية أو التأثير. ويُستخدم تحليل المخاطر لتقدير المخاطر بشكل كمي أو نوعي، حيث يُصنف كل خطر بحسب درجة خطورته (منخفض، متوسط، مرتفع، شديد)، ويُحدد مستوى الأولوية للتعامل معه. وتتضمن منهجيات تقدير المخاطر استخدام

المصـفوفات التصـنيفية (Risk Matrices) التي تجمع بين الاحتمالية والتأثير في جدول تصـنيفي، واستخدام النماذج الكمية التي تعطي أرقاماً تقديرية للخطر، وتحليل شـجرة الأخطاء والأحداث لتقدير احتمالية سيناريوهات معينة، واستخدام المؤشرات المركبة التي تجمع عوامل متعددة في تقدير واحد، والاسـتفادة من البيانات التاريخية عن حوادث مماثلة في منشـــآت شـــبيهة. ويُنتج عن هذه العملية قائمة أولويات للمخاطر، تحدد المخاطر التي تتطلب تدخلاً فورياً، وتلك التي يمكن التعامل معها بخطط طويلة الأجل، والمخاطر التي يُمكن قبولها ضـــمن الحدود المســـموحة. وتُعد هذه الأولويات بمثابة خريطة طريق لإدارة الموارد الأمنية وتوجيه الجهود نحو المناطق الأكثر حاجة، مع العلم أن تحليل المخاطر ليس عملية لمرة واحدة، بل يحتاج إلى تحديث دوري لمواكبة التغيرات في التهديدات ونقاط الضعف والأصول "5".

خامساً: استراتيجيات التعامل مع المخاطر (الاستجابة للمخاطر)

بعد تحديد المخاطر وتقديرها، يأتي دور اختيار الاســـتراتيجيات المناســـبة للتعامل معها، والتي تتنوع عادة بين خمس اســـتراتيجيات رئيســـية يمكن تطبيقها منفردة أو مجتمعة بحسـب طبيعة الخطر وإمكانيات المنشـأة. وتتمثل الاسـتراتيجية الأولى في تجنب المخاطر، وتقضـي بإلغاء النشـاط أو الأصـل أو الإجراء الذي يولّد الخطر، أو تعديله بشـكل يزيل الخطر تماماً، وتُسـتخدم هذه الاسـتراتيجية مع المخاطر الشـديدة التي لا يمكن السـيطرة عليها بوســائل أخرى. أما الاســتراتيجية الثانية فهي تقليل المخاطر، وتُعد الأكثر شـيوعاً، وتقوم على تطبيق إجراءات وقائية وعلاجية تخفض من احتمالية وقوع الخطر أو من حجم تأثيره، كتركيب أنظمة إنذار وكاميرات، أو تعزيز التدريب الأمني، أو تحسـين السـياسـات والإجراءات. وتتمثل الاسـتراتيجية الثالثة في نقل المخاطر، وتقضـــي بتحويل الخطر أو جزء منه إلى جهة أخرى، كالتأمين على الأصـول ضـد المخاطر، أو التعاقد مع شـركات أمن متخصـصـة، أو توزيع بعض العمليات على مواقع بديلة. أما الاســـتراتيجية الرابعة فهي قبول المخاطر، وتُسـتخدم للمخاطر المنخفضـة التي لا تبرر تكلفة معالجتها، أو للمخاطر

التي تفوق تكلفة معالجتها قيمة الأصل نفسه، وتتضمن مراقبة الخطر وقبوله ضمن حدود معينة مع الاستعداد للتعامل مع عواقبه. والاستراتيجية الخامسة هي استغلال المخاطر، وهي استراتيجية أقل شيوعاً في السياقات الأمنية التقليدية، وتُستخدم في سياقات محددة حيث قد يحمل الخطر فرصة إيجابية يمكن استغلالها، كاستغلال ثغرة في أمن منافس مثلاً. وتُنفذ هذه الاستراتيجيات من خلال خطط عمل محددة تحدد الإجراءات والموارد والمسؤوليات والجداول الزمنية، مع مراعاة أن اختيار الاستراتيجية المناسبة يتطلب موازنة دقيقة بين تكلفة تنفيذها وفعاليتها المتوقعة في تقليل الخطر، وبين الآثار الجانبية المحتملة لأي إجراء أمني على عمليات المنشأة وثقافتها التنظيمية."6"

سادساً: تطبيق الضوابط الأمنية

تُمثل الضوابط الأمنية الأدوات العملية التي تُنفذ بها استراتيجيات التعامل مع المخاطر، وهي تشمل مجموعة واسعة من الإجراءات والأنظمة والسياسات التي تهدف إلى تقليل المخاطر إلى مستويات مقبولة. وتُصنف الضوابط الأمنية عادةً إلى ضوابط مادية (كالحواجز والأسوار والأقفال والإضاءة وكاميرات المراقبة)، وضوابط تقنية (كأنظمة التحكم بالدخول، وجدران الحماية، وأنظمة التشفير، وأجهزة كشف التسلل)، وضوابط إجرائية (كالسياسات الأمنية المكتوبة، وإجراءات التفتيش، وخطط الطوارئ، وبرامج التدريب)، وضوابط تنظيمية (كهيكل إدارة الأمن، وتوزيع المسؤوليات، وآليات الرقابة والتدقيق). ويُعد اختيار الضوابط المناسبة وتطبيقها عملية متوازنة تراعي فعالية الضابط في مواجهة الخطر، وتكلفته مقارنة بقيمة الأصل، وسهولة تطبيقه واستدامته، وتوافقه مع ثقافة المنشأة وعملياتها، وإمكانية قياس فعاليته. وتُنفذ الضوابط عادةً وفق خطة زمنية محددة تأخذ في الاعتبار الأولويات والموارد المتاحة، وتُشمل عملية التنفيذ توفير الموازنات المالية اللازمة، وشراء وتركيب الأنظمة والمعدات، وتدريب وتأهيل الكوادر البشرية، ووضع وتوثيق السياسات والإجراءات، واختبار الأنظمة والتحقق من عملها. ويُعد إشراك جميع المعنيين في عملية تطبيق الضوابط من العوامل الأساسية لنجاحها، إذ

يسـهم في بناء الالتزام والمسـؤولية المشـتركة، وتجنب المقاومة أو التجاهل التي قد تعرقل تنفيذ الإجراءات الأمنية."7"

سابعاً: المراقبة والمراجعة المستمرة

لا تتوقف عملية إدارة المخاطر عند تطبيق الضـوابط، بل تسـتمر من خلال عمليات المراقبة والمراجعة المسـتمرة التي تهدف إلى التأكد من فاعلية الإجراءات المتخذة، واكتشـاف أي تغيرات في بيئة المخاطر تسـتدعي تعديلها. وتشـمل المراقبة جمع وتحليل البيانات المتعلقة بالأداء الأمني بشـكل منتظم، ومتابعة مؤشـرات الأداء الرئيسـية كعدد الحوادث الأمنية، ووقت الاسـتجابة للطوارئ، ونسـبة الامتثال للسـياسـات الأمنية، وفعالية أنظمة الكشـف والإنذار، ومسـتوى رضـا العاملين عن الإجراءات الأمنية. وتشـمل المراجعة إجراء تقييمات دورية شـاملة لمنظومة إدارة المخاطر بأكملها، وتتضمن مراجعة صحة تقديرات المخاطر في ضوء التغيرات في التهديدات ونقاط الضـعف والأصـول، وتقييم كفاءة وفعالية الضـوابط المطبقة ومدى تحقيقها للأهداف المرجوة، وتحديد الثغرات أو القصـور في السياسـات والإجراءات، واسـتخلاص الدروس من الحوادث الأمنية التي وقعت (سـواء في المنشـأة نفسـها أو في منشـآت مشـابهة)، وتقييم التغيرات في البيئة الخارجية والداخلية التي قد تؤثر على المخاطر. وتُسـتخدم نتائج المراقبة والمراجعة لتحديث خطط إدارة المخاطر، وتعديل الضـوابط، وإعادة توزيع الموارد، وتحسـين السـياسـات والإجراءات، مما يضـمن أن تظل عملية إدارة المخاطر ديناميكية ومسـتجيبة للمتغيرات، لا جامدة أو متجاوزة بالزمن."8"

ثامناً: التواصل والإبلاغ في إدارة المخاطر

يُعد التواصـل والإبلاغ عن المخاطر والإجراءات المتخذة للتعامل معها عنصـراً حيوياً في نجاح أي نظام لإدارة المخاطر، إذ يضمن أن جميع الأطراف المعنية لديهم المعلومات اللازمة للقيام بأدوارهم، ويسـهم في بناء ثقافة أمنية مشـتركة، ويعزز الشفافية والمساءلة. وتشمل قنوات التواصل والإبلاغ التقارير الدورية للإدارة العليا عن حالة المخاطر والأداء الأمني، والإحاطات الأمنية للعاملين عن التهديدات الحالية

والإجراءات المطلوبة، وتبادل المعلومات مع الأجهزة الأمنية والجهات الحكومية ذات العلاقة، والتواصل مع المجتمع المحلي والشركاء والموردين حول الجوانب الأمنية ذات الاهتمام المشترك، والإبلاغ الفوري عن الحوادث الأمنية والاستجابة لها. وتُعد جودة المعلومات المبلغ عنها عاملاً حاسماً في فاعلية التواصل، إذ يجب أن تكون دقيقة وموضوعية وفي الوقت المناسب، ومصممة لتناسب احتياجات كل فئة من الفئات المستهدفة، مع مراعاة الحساسية والسرية عند الضرورة. ويُوصى بأن يكون التواصل الأمني عملية تفاعلية وليست أحادية الاتجاه، بحيث تسمح بتلقي الملاحظات والأسئلة والمقترحات من جميع المستويات، مما يسهم في تحسين جودة إدارة المخاطر وتعزيز الشعور بالملكية والالتزام لدى جميع العاملين."9"

تاسعاً: تطبيق منهجيات إدارة المخاطر (نظرة تطبيقية)

تُطبق منهجيات إدارة المخاطر الأمنية في المنشآت الحيوية وفق نماذج معيارية متعارف عليها دولياً، من أبرزها نموذج إدارة المخاطر وفق المواصفة الدولية (ISO 31000)، الذي يقدم إطاراً عاماً ينطبق على مختلف أنواع المخاطر، ويؤكد على دمج إدارة المخاطر في الحوكمة والاستراتيجية والتخطيط، ويشجع على التخصيص وفقاً لسياق المنشأة وثقافتها. ويُستخدم أيضاً نموذج (NIST SP 800-30)الذي يقدم منهجية تفصيلية لتقييم المخاطر في الأنظمة المعلوماتية، مع تركيز خاص على المخاطر السيبرانية، ويُعد مرجعاً مهماً للمنشآت التي تعتمد بشكل كبير على التقنية. وتُطبق هذه المنهجيات عبر دورات متكررة تبدأ بتحديد السياق، ثم تقييم المخاطر (تحديد، تحليل، تقدير)، ثم معالجة المخاطر، ثم المراقبة والمراجعة، وأخيراً التواصل والتشاور. وتتميز المنهجيات الفعالة بمرونتها وقابليتها للتكيف مع خصوصية كل منشأة، وقدرتها على التعامل مع درجات متفاوتة من عدم اليقين، وتوفيرها لأدوات قابلة للقياس تساعد في اتخاذ القرارات، مع إمكانية دمجها مع أنظمة الإدارة الأخرى كالجودة والسلامة والبيئة. ويُنصح باستشارة خبراء متخصصين في اختيار وتطبيق المنهجيات المناسبة، وتدريب الكوادر الداخلية على

استخدامها، مع الأخذ في الاعتبار أن المنهجية وحدها لا تكفي، بل لا بد من الالتزام التنظيمي والدعم القيادي لضمان نجاحها واستدامتها."10"

عاشراً: إدارة المخاطر الناشئة

تواجه المنشآت الحيوية في العصر الحالي مخاطر ناشئة لم تكن موجودة أو لم تكن بالحدة نفسها في الماضي، وتتطلب أساليب جديدة في التعامل معها لا تستند بالضرورة إلى الخبرات التاريخية وحدها. وتشمل هذه المخاطر الناشئة الهجمات السيبرانية المتقدمة التي تستخدم تقنيات الذكاء الاصطناعي والتعلم الآلي، وهجمات الطائرات المسيرة التي أصبحت أكثر انتشاراً وقدرة، والتهديدات البيولوجية والوبائية كالجوائح التي قد تعطل سلاسل التوريد والعمليات، والمخاطر المناخية المتزايدة كالفيضانات وارتفاع درجات الحرارة وندرة المياه، والمخاطر الجيوسياسية كالحروب التجارية والعقوبات والصراعات الإقليمية، والمخاطر التكنولوجية المرتبطة بالاعتماد المتزايد على الأتمتة والأنظمة المستقلة. وتتطلب إدارة المخاطر الناشئة نهجاً استباقياً يعتمد على استشراف المستقبل وتحليل السيناريوهات المحتملة، والاستثمار في البحث والتطوير لفهم طبيعة هذه المخاطر وآليات عملها، وبناء القدرات التنظيمية والتقنية اللازمة للتعامل معها، وتطوير شراكات مع المؤسسات الأكاديمية والبحثية والجهات الحكومية المختصة. ويُعد بناء المرونة التنظيمية من أهم استراتيجيات التعامل مع المخاطر الناشئة، بحيث تكون المنشأة قادرة على التكيف مع التغيرات المفاجئة والصدمات غير المتوقعة، والتعلم من الأحداث والتطور بسرعة لتجاوز التحديات الجديدة، مع الحفاظ على استمرارية العمليات الحيوية في جميع الظروف."11"

وتشكل إدارة المخاطر الأمنية عملية متكاملة وديناميكية تتطلب التزاماً مستمراً من جميع مستويات المنشأة، بدءاً من الإدارة العليا التي يجب أن تضع الأمن كأولوية استراتيجية وتوفر الموارد اللازمة، وصولاً إلى كل عامل يجب أن يدرك دوره في الحفاظ على أمن المنشأة والإبلاغ عن أي ممارسات مشبوهة. وعندما تُمارس إدارة المخاطر بفعالية، فإنها لا تحمي المنشأة من الخسائر والأضرار فحسب، بل تسهم

أيضاً في تعزيز الثقة بين العاملين والعملاء والشركاء، وتحسين الكفاءة التشغيلية من خلال تحديد أولويات الاستثمارات الأمنية، ودعم اتخاذ القرارات الاستراتيجية من خلال توفير صورة واضحة عن بيئة المخاطر، كما أنها تُسهم في بناء سمعة المنشأة ككيان آمن وموثوق، وهو ما يشكل ميزة تنافسية في حد ذاته."12"

تحديد المخاطر الأمنية المحتملة

يُعد تحديد المخاطر الأمنية المحتملة الخطوة التأسيسية والأكثر حسماً في عملية إدارة المخاطر الأمنية، إذ تتوقف عليها سلامة وكفاءة جميع الخطوات اللاحقة من تحليل وتقدير ومعالجة ومراقبة. فما لم تُحدد المخاطر بدقة وشمولية، فإن الجهود المبذولة في معالجتها قد تكون موجهة نحو أهداف خاطئة أو غير كافية، مما يُخل بتوزيع الموارد ويُبقي المنشأة عرضة لمخاطر لم تُكتشف. وتستند عملية تحديد المخاطر إلى منهجية منظمة تجمع بين الدراسة الاستباقية للتهديدات المحتملة، وتحليل نقاط الضعف القائمة، وتقييم الأصول المعرضة للخطر، مع الاستفادة من الخبرات السابقة والدروس المستفادة من حوادث مشابهة في منشآت أخرى. وتُعد هذه العملية ديناميكية بطبيعتها، فلا تُجرى لمرة واحدة، بل تُكرر بشكل دوري أو كلما طرأت تغيرات جوهرية على المنشأة أو بيئتها التشغيلية، لضمان استمرار مواكبتها لتطور بيئة التهديدات."1"

أولاً: منهجية تحديد المخاطر الأمنية

تعتمد عملية تحديد المخاطر الأمنية على منهجية ثلاثية الأبعاد تربط بين الأصول والتهديدات ونقاط الضعف، إذ لا يُمكن تحديد الخطر بمعزل عن أي من هذه العناصر الثلاثة. فالخطر الأمني يُعرّف بأنه "إمكانية تعرض أصل ذي قيمة لضرر نتيجة لاستغلال تهديد معين لنقطة ضعف موجودة". وتُجرى عملية التحديد وفق خطوات منهجية متسلسلة، تبدأ بجرد شامل للأصول وتصنيفها وفق أهميتها وقيمتها، ثم تحديد جميع التهديدات المحتملة التي قد تستهدف هذه الأصول (طبيعية، بشرية، تكنولوجية)، ثم تحليل نقاط الضعف في الحماية القائمة التي قد تجعل الأصول عرضة للتهديدات، وأخيراً ربط هذه العناصر الثلاثة معاً لتحديد المخاطر الفعلية. وتُستخدم في هذه العملية مجموعة متنوعة من المصادر والأدوات، كالاستعانة بالخبرات الداخلية والخارجية، وتحليل البيانات التاريخية، ودراسة حالات المنشآت المماثلة، وتطبيق قوائم التدقيق الأمني المعيارية، وإجراء المقابلات مع العاملين في مختلف المستويات، وعقد جلسات العصف الذهني مع الفرق الأمنية، والاستفادة من

التقارير الاستخبارية والتحذيرية الصادرة عن الجهات المختصة. ويُوصى بإشراك ممثلين عن مختلف الإدارات والأقسام في عملية تحديد المخاطر، لضمان شمولية الرؤية واكتشاف المخاطر التي قد لا تكون واضحة للفريق الأمني وحده، مع الاستعانة بخبراء خارجيين متخصصين في المجالات التقنية أو التشغيلية المعقدة عند الحاجة."2"

ثانياً: مصادر المعلومات لتحديد المخاطر

تتنوع مصادر المعلومات التي يُعتمد عليها في تحديد المخاطر الأمنية، وتشمل مصادر داخلية وخارجية، رسمية وغير رسمية، تاريخية واستشرافية. وتشمل المصادر الداخلية سجلات الحوادث الأمنية السابقة في المنشأة، وتقارير التدقيق والمراجعة الداخلية، واستبيانات ومقابلات العاملين، ونتائج التفتيش والتدريبات الأمنية، وخطط الطوارئ والاستمرارية، وملاحظات الدوريات الأمنية، وتقارير الصيانة للأجهزة والأنظمة الأمنية. أما المصادر الخارجية فتشمل تقارير الجهات الأمنية والاستخباراتية الوطنية، ومنشورات المنظمات الدولية كالإنتربول والمنظمة الدولية للمعايير، وتقارير الشركات الأمنية الاستشارية، وتحليل الحوادث الأمنية في منشآت مماثلة، والتقارير الإعلامية الموثوقة عن التهديدات الناشئة، والمعلومات المتاحة عبر المنصات المتخصصة في أمن البنى التحتية. وتُعد الاستفادة من قاعدة معرفية واسعة ومتنوعة أمراً حيوياً لضمان عدم إغفال أي مخاطر محتملة، خاصة تلك التي لم تظهر بعد في المنشأة ولكنها قد تكون ظهرت في سياقات مشابهة. ويُوصى بإنشاء نظام لإدارة المعلومات الأمنية يقوم بجمع وتنظيم وتحليل هذه المصادر المختلفة، وتوزيع المعلومات ذات الصلة على المعنيين في الوقت المناسب، مما يُسهم في تحسين جودة وكفاءة عملية تحديد المخاطر بشكل مستمر "3".

ثالثاً: تصنيف المخاطر الأمنية

يُعد تصنيف المخاطر الأمنية أداة تنظيمية مهمة تُسهم في فهم طبيعة المخاطر وتحديد أولوياتها واختيار استراتيجيات التعامل المناسبة مع كل فئة. وتُصنف

المخاطر الأمنية عادة وفق معايير متعددة، منها مصـــدر الخطر) طبيعي، بشـــري متعمد، بشـــري غير متعمد، تكنولوجي، بيئي)، وطبيعة التأثير (مادي، معلوماتي، سماتي، تشغيلي، مالي)، ومجال التأثير (داخلي يقتصر على المنشأة، خارجي يمتد إلى المجتمع أو الدولة)، وزمن التأثير (فوري، قصـــير المدى، طويل المدى، تراكمي). ويُســـتخدم هذا التصـــنيف لتجميع المخاطر المتشـــابهة والتعامل معها بمنهجيات موحدة، ولتوجيه جهود التحديد نحو الفئات التي قد تكون مهملة أو غير مُغطاة بشكل كافٍ. كما يُساعد التصنيف في عملية التواصل والإبلاغ عن المخاطر، إذ يُتيح تقديم صورة واضحة ومنظمة لصناع القرار والجهات المعنية، بدلاً من تقديم قائمة طويلة ومبعثرة من المخاطر يصعب استيعابها. ويُوصى بأن يكون التصنيف مرناً وقابلاً للتطوير، بحيث يستوعب أنواعاً جديدة من المخاطر قد تظهر مع تطور التهديدات والتقنيات، وألا يُســـتخدم كقيد جامد يمنع النظر إلى المخاطر التي قد لا تندرج تماماً ضمن الفئات المحددة "٤".

رابعاً: تحديد المخاطر المادية والبنائية

تتعلق المخاطر المادية والبنائية بالتهديدات التي قد تلحق الضـرر بالأصـول المادية للمنشأة كالمباني والمعدات والمنشآت، وتشمل مجموعة واسعة من الاحتمالات التي يتعين فحصـها بدقة. وتشـمل هذه المخاطر الحرائق والانفجارات الناتجة عن أعطال كهربائية أو تسـربات غازية أو مواد قابلة للاشـتعال، والانهيارات الهيكلية الناجمة عن سـوء التصـميم أو التآكل أو الأحمال الزائدة، والأضـرار الناجمة عن الكوارث الطبيعية كالزلازل والفيضـانات والعواصـف، والتخريب المادي كتكسـير النوافذ أو إتلاف المعدات، والسـرقة أو النهب للمواد والمعدات الثمينة، والتسـريبات الكيميائية أو الإشـعاعية من عمليات التخزين أو التشـغيل. ويُحدد كل خطر من هذه المخاطر من خلال مسح ميداني شـامل للمنشـأة، ومراجعة المخططات الهندسـية ومواصـفات البناء، وتقييم حالة البنية التحتية وعمرها الافتراضـي، وتحليل سـجلات الصـيانة والأعطال السـابقة، ودراسـة البيئة المحيطة واحتمالية تعرضـها للكوارث الطبيعية، ومراجعة إجراءات التعامل مع المواد الخطرة وتخزينها. ويُوصـى بإشراك مهندسين

متخصـــصـــين في هذه العملية، خاصـــة في المنشـــآت المعقدة أو القديمة، وإجراء اختبارات دورية لســـلامة المباني والمنشـــآت، وتحديث ســـجلات المخاطر المادية باستمرار لتعكس أي تغيرات في حالة البنية التحتية أو في البيئة المحيطة بها."5"

خامساً: تحديد المخاطر البشرية

تُعد المخاطر البشـــرية من أكثر أنواع المخاطر تعقيداً وتنوعاً، إذ تشـــمل جميع التهديدات التي ينشئها أو يتسبب فيها العنصر البشري، سواء بقصد أو بدون قصد. وتشمل المخاطر البشرية المتعمدة الأعمال الإرهابية كالتفجيرات والهجمات المسلحة والاختطاف، والتخريب المتعمد للمعدات والأنظمة، والســـرقة الداخلية والخارجية، والتجسس الصناعي وسرقة المعلومات الحساسة، والهجمات السيبرانية الموجهة التي ينفذها قراصنة أو جماعات إجرامية أو دول معادية، والتسلل إلى المنشأة بقصد الإضرار بها، والابتزاز والتهديد ضد العاملين أو الإدارة. أما المخاطر البشرية غير المتعمدة فتشمل الأخطاء التشغيلية كالضغط على أزرار خاطئة أو إغفال إجراءات السلامة، والإهمال في اتباع السياسات والإجراءات الأمنية كترك الأبواب مفتوحة أو مشـــاركة كلمات المرور، ونقص التدريب وعدم المعرفة الكافية بالإجراءات الأمنية، والإرهاق والضـــغوط النفســـية التي قد تؤدي إلى أخطاء أو ردود فعل غير محسوبة، وضعف الوعي الأمني وعدم الإبلاغ عن الممارسات المشبوهة، والأخطاء في التعامل مع المواد الخطرة أو الأنظمة الحساسة. ويُحدد هذا النوع من المخاطر من خلال تحليل الســـلوكيات والأنماط الوظيفية، وتقييم مســـتويات التدريب والوعي الأمني، ومراجعة سجلات الحوادث والأخطاء السابقة، وإجراء مقابلات مع العاملين لفهم التحديات التي يواجهونها، وتطبيق اختبارات دورية لقياس مدى اســـتيعابهم للإجراءات الأمنية. كما يُوصـــى بإجراء تحليل للثقافة التنظيمية لتحديد ما إذا كانت تشـــجع على الإبلاغ عن الأخطاء والمخاطر، أم أنها تُثبط المبادرة وتدفع لإخفاء الأخطاء، مما قد يفاقم المخاطر البشرية بشكل كبير."6"

سادساً: تحديد المخاطر التقنية والرقمية

مع تزايد الاعتماد على التقنية في إدارة المنشآت الحيوية، أصبحت المخاطر التقنية والرقمية تحتل موقعاً متقدماً في قائمة المخاطر الأمنية، وتتطلب أساليب متخصصة لتحديدها وتقييمها. وتشمل هذه المخاطر الهجمات السيبرانية كالاختراقات وبرامج الفدية وهجمات حجب الخدمة والتصيد الإلكتروني، وأعطال الأنظمة كانهيار الخوادم أو تعطل الشبكات أو توقف أنظمة التحكم الصناعية، وثغرات البرمجيات التي لم تُصحح بعد، وضعف التشفير أو استخدام بروتوكولات أمنية قديمة، وسرقة البيانات أو تسريبها نتيجة اختراق أو إهمال، وهجمات الهندسة الاجتماعية التي تستهدف العاملين للحصول على معلومات حساسة، وتقادم الأجهزة والبرمجيات وعدم توافقها مع متطلبات الأمن الحديثة، والاعتماد على موردين أو خدمات سحابية غير مؤمنة بشكل كافٍ. ويُحدد هذا النوع من المخاطر من خلال عمليات تدقيق تقنية شاملة، واختبارات اختراق دورية للأنظمة، ومراجعة سجلات الأمن السيبراني وتحليل الحوادث السابقة، وتقييم مدى تطبيق أفضل الممارسات في أمن المعلومات، وفحص سلاسل التوريد التقنية لتحديد أي ثغرات محتملة، وتحليل المخاطر المرتبطة بتقنيات الذكاء الاصطناعي والأتمتة والإنترنت الصناعي للأشياء. ويُوصى بأن يشارك في هذه العملية خبراء متخصصون في الأمن السيبراني وأمن نظم التحكم الصناعية، وأن تُجرى هذه التقييمات بشكل متكرر نظراً للوتيرة السريعة لتطور التهديدات التقنية والرقمية."7"

سابعاً: تحديد المخاطر التنظيمية والإدارية

تتعلق المخاطر التنظيمية والإدارية بالهيكل الإداري للمنشأة وسياساتها وإجراءاتها وثقافتها، وكيف يمكن أن تشكل هذه العوامل مصادر للخطر أو عوامل مضاعفة لمخاطر أخرى. وتشمل هذه المخاطر ضعف هيكل إدارة الأمن وعدم وضوح الصلاحيات والمسؤوليات، وغموض السياسات الأمنية أو عدم تحديثها بشكل دوري، وضعف التنسيق بين الإدارات والأقسام المختلفة، ونقص الموارد المالية والبشرية المخصصة للأمن، وضعف آليات الرقابة والتدقيق الداخلي، وغياب خطط الطوارئ واستمرارية العمل، وضعف آليات الإبلاغ عن المخاطر والحوادث، وعدم

كفاية التدريب والتأهيل للعاملين في المجال الأمني، وغياب ثقافة الأمن التنظيمية وعدم إشراك العاملين في الجهود الأمنية، والاعتماد المفرط على أفراد معينين دون تخطيط للخلافة أو التناوب. ويُحدد هذا النوع من المخاطر من خلال مراجعة الهيكل التنظيمي وسياسات المنشأة، وإجراء مقابلات مع الإدارة والعاملين في مختلف المستويات لفهم التحديات الإدارية، وتقييم مدى فعالية آليات الرقابة والتدقيق، ومراجعة ميزانيات الأمن وتوزيعها، وتقييم برامج التدريب والتوعية الأمنية ومدى انتشارها وتأثيرها. ويُوصى بإشراك مستشارين إداريين متخصصين في هذه المراجعات، لأن المخاطر التنظيمية غالباً ما تكون غير مرئية للعاملين داخل المنشأة الذين اعتادوا على الوضع القائم، كما يُوصى بمراجعة هذه المخاطر كلما طرأت تغيرات إدارية أو تنظيمية كبيرة على المنشأة."8"

ثامناً: تحديد المخاطر الخارجية والبيئية

تشمل المخاطر الخارجية والبيئية جميع التهديدات التي تنشأ من خارج المنشأة، والتي تقع غالباً خارج نطاق السيطرة المباشرة للإدارة ولكن يمكن التخفيف من آثارها من خلال الاستعداد الجيد. وتشمل هذه المخاطر الكوارث الطبيعية كالزلازل والفيضانات والأعاصير والجفاف والحرائق الطبيعية، والأحداث الجيوسياسية كالحروب والنزاعات والعقوبات الاقتصادية وعدم الاستقرار السياسي، والأزمات الاقتصادية التي قد تؤثر على تمويل العمليات أو سلاسل التوريد، والأوبئة والجوائح الصحية التي قد تعطل حضور العاملين وسلاسل الإمداد، والتغيرات المناخية طويلة المدى التي قد تؤثر على توافر الموارد أو كفاءة العمليات، والحوادث في المنشآت المجاورة كالانفجارات أو التسربات الكيميائية، والاضطرابات الاجتماعية كالاحتجاجات وأعمال الشغب التي قد تهدد محيط المنشأة، والتغيرات التشريعية والقانونية التي قد تفرض متطلبات أمنية جديدة أو تحد من بعض الممارسات. ويُحدد هذا النوع من المخاطر من خلال دراسة البيئة المحيطة بالمنشأة وتحليل المخاطر الطبيعية والجيوسياسية في المنطقة، ومتابعة التطورات الاقتصادية والسياسية والقانونية ذات الصلة، والاستفادة من تقارير الهيئات المختصة كمراكز الأرصاد

الجوية وهيئات المسح الجيولوجي ومراكز الدراسات الاستراتيجية، وإقامة علاقات مع السلطات المحلية والمنشآت المجاورة لتبادل المعلومات حول المخاطر المشتركة. ويُوصـــى بإجراء تحليلات ســـيناريوهات متعددة للمخاطر الخارجية، لتقدير الآثار المحتملة على المنشأة في مختلف الأحوال، وتطوير خطط استجابة مرنة تتناسب مع مختلف السيناريوهات."9"

تاسعاً: تحديد المخاطر المتتالية والمترابطة

تتميز المنشــآت الحيوية بشـبكة معقدة من الترابطات الداخلية والخارجية، مما يجعل بعض المخاطر قادرة على التسبب في سلسلة من التأثيرات المتتالية التي قد تمتد إلى ما هو أبعد من الهدف المباشـــر للخطر. وتشـــمل هذه المخاطر المتتالية أن يؤدي حادث في نظام كهربائي إلى تعطل أنظمة التبريد، مما يؤدي إلى ارتفاع حرارة المعدات وتعطل أنظمة التحكم، ومن ثم توقف الإنتاج أو الخدمة، وقد يمتد التأثير إلى منشــآت أخرى تعتمد على تلك الخدمة. كما قد يؤدي هجوم سـيبراني على نظام مالي إلى شـلل المدفوعات، مما يؤثر على قدرة المنشـأة على شـراء المواد الخام أو دفع رواتب العاملين، ويؤدي في النهاية إلى توقف العمليات. وتُحدد هذه المخاطر من خلال تحليل الترابطات بين مختلف الأنظمة والعمليات في المنشـــأة، ورســـم خرائط التبعيات بين الأصول والخدمات، وتحليل سيناريوهات متعددة لانتشار الأثر، واستخدام نماذج المحاكاة لتقدير سرعة ومدى انتشـار التأثيرات. ويُوصـى بإشـراك خبراء من مختلف التخصصـات في هذه العملية، لفهم طبيعة الترابطات بين الأنظمة المختلفة، وتحديد نقاط الانهيار الحرجة التي قد تؤدي إلى تأثيرات متتالية واســـعة النطاق، وتركيز جهود الحماية على هذه النقاط لقطع سـلسـلة التأثيرات المتتالية قبل أن تنتشر."10"

عاشراً: توثيق المخاطر وتحديثها باستمرار

يُعد توثيق المخاطر المحددة بشـكل منهجي ودقيق من الخطوات الأسـاسـية لضـمان استمرارية وفعالية عملية إدارة المخاطر، إذ يُتيح الرجوع إلى قاعدة بيانات المخاطر عند الحاجة، ويُســـهل عمليات التقييم والمراجعة والتحديث، ويُســـهم في التواصـــل

الفعال مع جميع المعنيين حول طبيعة المخاطر وأولوياتها. وتشـــمل عملية التوثيق تسجيل كل خطر بتفاصيله الأساسية كاسم الخطر ووصفه ومصدره، والأصول المعرضـــة له، ونقاط الضـــعف التي يســـتغلها، والأســـباب المحتملة لوقوعه، والســـيناريوهات المحتملة لتطوره، وتقديرات أولية لاحتماليته وتأثيره، والإجراءات الحالية للتعامل معه. ويُوصى باستخدام قواعد بيانات إلكترونية متخصصة في إدارة المخاطر، تُتيح التحديث الســـهل والبحث المتقدم وإعداد التقارير، مع وضـــع نظام للتحكم في الإصـــدارات والتغييرات يضـــمن تتبع تاريخ كل خطر والتعديلات التي طرأت عليه. وتُحدث ســجلات المخاطر بشــكل دوري، إما وفق جدول زمني محدد (كمراجعة ســنوية أو نصــف ســنوية)، أو عند وقوع حوادث أمنية تســتدعي إعادة التقييم، أو عند حدوث تغيرات جوهرية في المنشـأة (كتوسـع في العمليات، أو إدخال تقنيات جديدة، أو تغير في البيئة الخارجية)، أو عند ظهور تهديدات جديدة تســتدعي إعادة النظر في المخاطر القائمة. ويُعد تحديث ســـجلات المخاطر عملية مســـتمرة وليسـت حدثاً منفصـلاً، ويجب أن تندرج ضـمن الممارسـات اليومية للفريق الأمني، بحيث يُســـجل أي خطر جديد فور اكتشـــافه، وتُحدث تقديرات المخاطر القائمة بناءً على المعلومات الجديدة."11"

وتُعد عملية تحديد المخاطر الأمنية المحتملة حجر الزاوية في أي نظام فعال لإدارة المخاطر في المنشـآت الحيوية، وكلما كانت هذه العملية أكثر شـمولاً ودقة وتحديثاً، كلما كان النظام الأمني أكثر قدرة على حماية الأصول واستمرارية العمليات. ويجب أن ينظر إلى تحديد المخاطر على أنه اســتثمار اســتراتيجي وليس تكلفة إضـــافية، فالوقت والجهد المبذولان في تحديد المخاطر بدقة يوفران موارد أكبر مما يستهلكان، من خلال توجيه الاســتثمارات الأمنية نحو الأولويات الحقيقية، وتجنب الإنفاق على تدابير غير فعالة أو غير ضـرورية. وتظل عملية تحديد المخاطر مسؤولية مشـتركة بين جميع مسـتويات المنشـأة، وتتطلب ثقافة أمنية متجذرة تشـجع على الإبلاغ عن المخاطر والإسهام في تحسين فهمها ومعالجتها."12"

تقييم مستوى المخاطر الأمنية

يُعد تقييم مستوى المخاطر الأمنية المرحلة المنهجية التي تلي تحديد المخاطر المحتملة، وتتمثل مهمتها الأساسية في تحويل قائمة المخاطر النوعية إلى تقديرات كمية أو شبه كمية تُمكن من ترتيب الأولويات واتخاذ القرارات الرشيدة بشأن تخصيص الموارد واختيار استراتيجيات المعالجة. فالتحديد وحده لا يكفي، إذ قد تكون قائمة المخاطر طويلة ومتنوعة، ولا يتسع الوقت أو الموارد لمعالجتها جميعاً بنفس المستوى، مما يستوجب عملية تقييم دقيقة تُميز بين المخاطر ذات الأولوية القصوى وتلك التي يمكن قبولها أو تأجيل معالجتها. وتقوم عملية تقييم المخاطر على تحليل متغيرين رئيسيين: احتمال وقوع الخطر، وحجم تأثيره في حال وقوعه، مع الأخذ في الاعتبار نقاط الضعف القائمة التي قد تزيد من أي من المتغيرين. وتُستخدم مخرجات التقييم لتوليد "خريطة مخاطر" تُصنف المخاطر وفق درجاتها، وتُوجه جهود المعالجة نحو المخاطر الأعلى درجة أولاً، مع مراعاة أن التقييم ليس عملية جامدة بل ديناميكية تتغير بتغير المعطيات، وتحتاج إلى تحديث مستمر لتعكس التطورات في بيئة التهديدات والضوابط الأمنية المطبقة."1"

أولاً: منهجيات تقييم المخاطر

تتنوع منهجيات تقييم المخاطر بين النوعية والكمية وشبه الكمية، ولكل منهجية خصائصها ومزاياها ومجالات استخدامها المناسبة. وتعتمد المنهجيات النوعية على الوصف والتصنيف، حيث يُصنف احتمال وقوع الخطر وتأثيره باستخدام مقياس لفظي كـ(منخفض، متوسط، مرتفع، شديد)، وتُستخدم هذه المنهجيات عندما تكون البيانات الكمية غير متوفرة أو عندما تكون المخاطر ذات طبيعة يصعب قياسها كمياً، كالمخاطر السماتية أو المخاطر الناشئة. وتتميز بسهولة تطبيقها وسرعتها، لكنها تفتقر إلى الدقة وقد تختلف تقديراتها بين مقيم وآخر. أما المنهجيات الكمية فتعتمد على الأرقام والنماذج الرياضية، حيث تُعطى قيمة عددية لاحتمال وقوع الخطر وتأثيره (كاحتمال ٠,٠١ وحجم خسارة مليون دولار)، وتُستخدم عندما تتوفر بيانات تاريخية كافية ونماذج إحصائية موثوقة، وتتميز بدقتها وقابليتها للمقارنة

الموضـوعية، لكنها تتطلب خبرة وبيانات قد لا تكون متاحة دائماً، خاصـة للمخاطر النادرة أو الجديدة. أما المنهجيات شـبه الكمية فتجمع بين النوعي والكمي، باسـتخدام مقاييس عددية للاحتمال والتأثير مع الاحتفاظ ببعض العناصـر النوعية، كاسـتخدام مقياس من ١ إلى ٥ لكل من الاحتمال والتأثير، ثم ضـربهما للحصـول على درجة الخطر. وتُعد هذه المنهجية الأكثر شـيوعاً في تطبيقات أمن المنشـآت، لكونها توازن بين الدقة وسهولة التطبيق، وتُمكن من ترتيب المخاطر دون الحاجة إلى بيانات كمية معقدة. ويُوصـى باختيار المنهجية المناسبة وفقاً لطبيعة المنشـأة وحجمها ومواردها، مع إمكانية استخدام أكثر من منهجية للمخاطر المختلفة، شريطة أن تكون المقارنات بين المخاطر متسقة ومبنية على أسس موحدة."2"

ثانياً: تقدير الاحتمالية

يُعد تقدير احتمالية وقوع الخطر أحد المتغيرين الأساسيين في تقييم المخاطر، ويعبّر عن مدى توقع حدوث الخطر خلال فترة زمنية محددة (كعام أو خمسـة أعوام). ويعتمد تقدير الاحتمالية على تحليل عدة عوامل، منها التاريخ الحوادثي للمنشـأة وما إذا كان خطر مشـابه قد وقع سـابقاً وتكرار حدوثه، وطبيعة التهديد ومدى نشـاط الجهات التي تمثله وقدراتها، ومدى تعرض المنشـأة لذلك التهديد بناءً على موقعها ونشـاطها وسـمعتها، وفعالية الضـوابط الأمنية الحالية في ردع أو منع ذلك الخطر، والمؤشـرات الاسـتباقية المتوفرة (كإنذارات اسـتخبارية أو تغيرات في بيئة التهديدات). وتُسـتخدم في تقدير الاحتمالية أدوات متعددة كتحليل البيانات التاريخية، وتحليل الاتجاهات، وتحليل السيناريوهات، وتقديرات الخبراء، والنماذج الإحصائية، وأحياناً تقنيات المحاكاة الحاسـوبية للسـيناريوهات المعقدة. ويُعبّر عن الاحتمالية إما بشـكل نوعي (كالقليل جداً، القليل، المتوسـط، الكثير، الكثير جداً) أو كمي (كاحتمال ٠,٠٥ أي ٥٪ خلال عام)، أو شـبه كمي (كدرجة ١ إلى ٥). ويُنبه إلى ضـرورة توخي الحذر في تقدير الاحتمالية، إذ تميل الفرق الأمنية أحياناً إلى المبالغة في تقدير احتمالية المخاطر المألوفة والتقليل من احتمالية المخاطر النادرة أو غير المألوفة، مما قد يؤدي إلى انحراف في الأولويات. ويُوصـى بالاستعانة بمصادر متعددة للتثبت

من تقديرات الاحتمالية، وتحديثها باستمرار كلما توفرت معلومات جديدة تؤثر عليها."3"

ثالثاً: تقدير التأثير

يمثل تقدير تأثير الخطر المتغير الثاني الأساسي في تقييم المخاطر، ويعبّر عن حجم الضرر المتوقع في حال وقوع الخطر، ويُقاس بأبعاد متعددة تتجاوز الجانب المالي لتشمل الجوانب البشرية والتشغيلية والسماتية والقانونية. وتشمل أبعاد التأثير التأثير البشري كالإصابات والوفيات والأضرار الصحية للعاملين والزوار، والتأثير المالي كتكاليف الإصلاح والاستبدال، وفقدان الإيرادات، والتعويضات والغرامات، والتأثير التشغيلي كتوقف العمليات الحيوية وفقدان القدرة الإنتاجية، والتأثير السماتي كضرر سمعة المنشأة وفقدان ثقة العملاء والشركاء، والتأثير القانوني والتنظيمي كالمخالفات القانونية والغرامات والملاحقات القضائية، والتأثير البيئي كالتلوث والأضرار البيئية، والتأثير الاستراتيجي كتأثير الحادث على القدرة التنافسية أو الأمن القومي. ويُستخدم في تقدير التأثير مجموعة من الأدوات كتحليل التكلفة والعائد، ونماذج تقدير الخسائر، وتحليل السيناريوهات الأسوأ، وتقارير الحوادث المماثلة في منشآت أخرى، وتقديرات الخبراء في المجالات المتخصصة. ويُعبّر عن التأثير إما نوعياً (كطفيف، متوسط، كبير، كارثي) أو كمياً (كقيمة خسارة متوقعة بالعملة، أو عدد أيام التوقف، أو عدد الإصابات المتوقعة) أو شبه كمي (كدرجة من ١ إلى ٥). ويُوصى بتقدير التأثير في عدة سيناريوهات (سيناريو محتمل، سيناريو متوسط، سيناريو أسوأ) لتوفير صورة أكثر شمولية عن المخاطر، وتحديث تقديرات التأثير كلما توفرت معلومات جديدة عن قيمة الأصول أو تكلفة التعطل أو المتغيرات الأخرى المؤثرة."4"

رابعاً: حساب درجة المخاطر (مصفوفة المخاطر)

تُستخدم مصفوفة المخاطر (Risk Matrix) كأداة شائعة وفعالة لدمج تقديرات الاحتمالية والتأثير في درجة واحدة للمخاطر، مما يُسهل تصنيف المخاطر وترتيب أولوياتها. وتتكون المصفوفة عادة من جدول ثنائي الأبعاد، حيث يمثل المحور

الأفقي مستويات الاحتمالية والمحور الرأسي مستويات التأثير، وتُحدد درجة الخطر عند تقاطع الصف والعمود. وتُقسّم المصفوفة عادة إلى مناطق لونية (كالأخضر للمخاطر المنخفضة، والأصفر للمتوسطة، والبرتقالي للمرتفعة، والأحمر للشديدة) لتيسير القراءة واتخاذ القرارات. ويتم حساب درجة الخطر إما بجمع أو ضرب درجات الاحتمال والتأثير، أو باستخدام خوارزميات أكثر تعقيداً تأخذ في الاعتبار عوامل إضافية كسرعة التفاقم وقابلية الاكتشاف. وتُستخدم المصفوفة لتوليد "خريطة حرارية للمخاطر" تُظهر توزيع المخاطر حسب درجاتها، وتُمكن من تحديد المخاطر التي تتطلب تدخلاً فورياً، وتلك التي يمكن جدولتها لاحقاً، والمخاطر التي يمكن قبولها ضمن الحدود المسموحة. ويُوصى بتخصيص المصفوفة لتناسب خصوصية كل منشأة، من خلال تحديد معايير الاحتمالية والتأثير بما يتناسب مع طبيعة نشاطها وحجمها وقدرتها على تحمل المخاطر، وتحديث المصفوفة دورياً لتعكس التغيرات في تلك المعايير، مع الأخذ في الاعتبار أن المصفوفة أداة مبسطة وقد لا تلتقط بعض التعقيدات، لذا يُنصح باستخدامها جنباً إلى جنب مع تحليلات أكثر تفصيلاً للمخاطر شديدة الأهمية."5"

خامساً: تحديد مستويات تحمل المخاطر (رغبة المخاطرة)

لا يمكن فهم درجة المخاطر بمعزل عن مستوى تحمل المنشأة للمخاطر (Risk Tolerance)، وهو مقدار الخطر الذي تكون المنشأة مستعدة لقبوله في سعيها لتحقيق أهدافها. ويختلف مستوى تحمل المخاطر بين منشأة وأخرى بحسب طبيعة نشاطها، ومواردها، والتزاماتها القانونية، وثقافتها التنظيمية، وتوقعات أصحاب المصلحة. وتُستخدم مستويات التحمل كمعيار لتحديد ما إذا كانت درجة مخاطر معينة مقبولة، أم تتطلب معالجة، أم غير مقبولة بتاتاً وتستوجب تجنب النشاط المسبب لها. وتُعبر مستويات التحمل عادة بحدود كمية أو نوعية، كأن تقرر المنشأة أنها لا تقبل أي خطر قد يؤدي إلى وفيات، أو أنها لا تقبل خسائر مالية تتجاوز نسبة معينة من رأس المال، أو أنها تقبل المخاطر المنخفضة والمتوسطة ولكن ليس المرتفعة. ويُوصى بأن يُحدد مستوى تحمل المخاطر من قبل الإدارة العليا، وأن

يُراجع دورياً للتأكد من ملاءمته للاســـتراتيجية العامة للمنشـــأة وبيئة المخاطر المتغيرة، وأن يُبلغ لجميع المعنيين ليكون مرشـــداً في عمليـات تقييم ومعـالجـة المخاطر، مع الأخذ في الاعتبار أن تحديد مســـتوى تحمل منخفض جداً قد يكلف المنشأة فرصـاً مهمة، في حين أن تحديد مستوى مرتفع جداً قد يعرضـها لمخاطر لا تحتمل."6"

سادساً: ترتيب أولويات المخاطر

تُعد عملية ترتيب أولويات المخاطر من أهم مخرجات التقييم، حيث توجه جهود المنشأة ومواردها نحو المخاطر الأكثر إلحاحاً وأشدها تأثيراً. ويتم ترتيب الأولويات بناءً على درجة المخاطر المحسـوبة، بحيث تُعطى الأولوية القصـوى للمخاطر ذات الدرجة الأعلى (شـــديدة أو مرتفعة)، وتنخفض الأولوية بتدرج الدرجة. ولكن قد تدخل عوامل أخرى في ترتيب الأولويات إلى جانب الدرجة، كســـرعة تفاقم الخطر (فبعض المخاطر تتحول من متوســـطة إلى كارثية بســـرعة كبيرة إذا لم تُعالج)، وقابلية المعالجة (فبعض المخاطر يُمكن معالجتها بســـرعة وبتكلفة منخفضـــة، مما يجعلها أولوية حتى لو كانت درجتها متوســـطة)، والترابطات (فبعض المخاطر قد تكون بوابـة لمخـاطر أخرى أكبر إذا لم تُعـالج)، والمتطلبـات القـانونيـة والتنظيميـة (فبعض المخاطر قد تكون درجة خطرها منخفضـــة ولكن القانون يلزم بمعالجتها). ويُنتج عن ترتيب الأولويات قائمة مرقمة بالمخاطر، تُحدد لكل خطر إطاراً زمنياً مقترحاً للمعالجة (كفوري، خلال ٣ أشـهر، خلال ٦ أشـهر، خلال عام)، وتُخصـص الموارد المالية والبشـرية وفقاً لهذه الأولويات. ويُوصـى بأن تُراجع قائمة الأولويات بشكل دوري، خاصـة بعد تنفيذ إجراءات معالجة أو عند تغير بيئة المخاطر، لضمان استمرار ملاءمتها وفعاليتها في توجيه الجهود الأمنية."7"

سابعاً: تقييم المخاطر المتبقية

بعد تحديد وتنفيذ إجراءات معـالجـة المخـاطر، يظهر مفهوم "المخـاطر المتبقيـة " (Residual Risk)، وهي المخـاطر التي تبقى قـائمـة بعـد تطبيق الضـــوابط والإجراءات الأمنية. ويُعد تقييم المخاطر المتبقية خطوة أســـاســـية للتأكد من أن

المعالجة قد خفضت الخطر إلى مستوى مقبول ضمن حدود تحمل المنشأة، ولتحديد ما إذا كانت هناك حاجة إلى معالجات إضـــافية. وتتم عملية تقييم المخاطر المتبقية بإعادة تطبيق منهجية تقييم المخاطر ذاتها، ولكن مع الأخذ في الاعتبار الضـــوابط الجديدة المطبقة، بحيث يُعاد تقدير الاحتمالية والتأثير في ضـــوء هذه الضـــوابط، وتُحســـب درجة الخطر الجديدة وتُقارن بالدرجة الأصـــلية لتحديد حجم التحســـن المحقق. فإذا كانت المخاطر المتبقية لا تزال أعلى من مستوى تحمل المنشـأة، فهذا يعني أن المعالجة غير كافية وتستوجب إعادة النظر فيها أو تطبيق ضوابط إضافية. أما إذا كانت المخاطر المتبقية ضمن المستوى المقبول، فيمكن قبولها مع الاستمرار في مراقبتها. ويُوصـــى بتوثيق نتائج تقييم المخاطر المتبقية، وتســـجيل الضـــوابط المطبقة وتأثيرها على درجة الخطر، لتكون مرجعاً في المراجعات المســـتقبلية، وتحديث سـجلات المخاطر لتعكس الوضـع الجديد، مع مراعاة أن المخاطر المتبقية ليســـت ثابتة، بل قد تتغير بتغير فعالية الضـــوابط أو بتغير بيئة التهديدات، مما يستوجب إعادة تقييمها بشكل دوري."8"

ثامناً: أدوات وتقنيات تقييم المخاطر

تتوفر مجموعة متنوعة من الأدوات والتقنيات التي تُســـهم في تحســـين دقة وكفاءة عملية تقييم المخاطر الأمنية، وتختلف هذه الأدوات في تعقيدها وتكلفتها ومناسبة كل منها لسياقات معينة. وتشمل هذه الأدوات برمجيات إدارة المخاطر المتخصصة التي توفر قوالب لتقييم المخاطر، وحســـابات آلية لدرجات المخاطر، وقواعد بيانات لتخزين المخاطر وتتبع معالجتها، وتوليد تقارير ورسـوم بيانية، وقد تتضـمن بعض هذه البرمجيات ميزات متقدمة كتحليل الســيناريوهات والمحاكاة. وتُســتخدم أدوات تحليل القرار كأشجار القرار ومصفوفات القرار لتقييم المخاطر في سياق الخيارات المتعددة، وأدوات التحليل الإحصـــائي كتحليل الانحدار وتحليل الســـلاســـل الزمنية لتقدير الاحتمالية بناءً على البيانات التاريخية، وأدوات العصف الذهني والاستبيانات لاســـتجلاء آراء الخبراء والعاملين في تقدير المخاطر، وتقنيات المحاكاة كمحاكاة مونت كارلو لتقدير توزيع الاحتمالات للمخاطر المعقدة. ويُوصـــى باختيار الأدوات

المناسـبة وفقاً لحجم المنشـأة وتعقيدها، ومواردها المالية والبشـرية، وخبرة الفريق الأمني، مع مراعاة أن الأداة الأكثر تعقيداً ليست بالضرورة الأفضل، بل الأنسب هو ما يُلبي الاحتياجات الفعلية بكفاءة وتكلفة معقولة، وأن يُسـتثمر في تدريب الفريق الأمني على استخدام الأدوات المختارة بشكل فعال."9"

تاسعاً: التحديات في تقييم المخاطر الأمنية

تواجه عملية تقييم المخاطر الأمنية في المنشـآت الحيوية مجموعة من التحديات التي ينبغي awareness بها والتعامل معها بحذر لضـمان سـلامة النتائج. ومن أبرز هذه التحديات عدم اليقين في تقدير الاحتمالية، خاصـة للمخاطر النادرة أو الجديدة التي لا تتوفر عنها بيانات تاريخية كافية، مما قد يؤدي إلى تقديرات غير دقيقة تعتمد على التخمين أو التقدير الشـخصـي أكثر من الأدلة الموضـوعية. ويُمثل التحيز البشري تحدياً آخر، حيث يميل المقيمون إلى المبالغة في تقدير المخاطر المألوفة لهم والتقليل من المخاطر غير المألوفة، أو التأثر بتجاربهم الشـخصـية أو بالحوادث الأخيرة التي حظيت بتغطية إعلامية واسـعة. كما تُمثل التغيرات السـريعة في بيئة التهديدات تحدياً كبيراً، إذ قد تصـبح تقديرات المخاطر قديمة بسـرعة، خاصـة في المجالات التقنية والأمن السيبراني التي تتطور بوتيرة متسارعة. ويُضاف إلى ذلك صـعوبة تقدير التأثيرات غير الملموسـة كالضـرر السـماتي أو فقدان الثقة، والتي يصـعب قياسـها كمياً ولكنها قد تكون أكثر تأثيراً من الخسـائر المادية المباشـرة. وللتغلب على هذه التحديات، يُوصى باستخدام مصادر متعددة للمعلومات، وإشراك خبراء متنوعين في عملية التقييم لتقليل التحيزات الفردية، وتحديث التقييمات بشـكل متكرر، واسـتخدام منهجيات مرنة تسـمح بإعادة التقدير عند توفر معلومات جديدة، وتوثيق الافتراضـات التي بُنيت عليها التقديرات لتكون قابلة للمراجعة والتصـحيح "10".

عاشراً: التكامل مع عمليات إدارة المخاطر الأخرى

لا تُعد عملية تقييم المخاطر الأمنية نشاطاً منعزلاً، بل هي جزء من منظومة متكاملة لإدارة المخاطر تشمل أيضاً تحديد المخاطر ومعالجتها ومراقبتها، ويجب أن تُصمم

وتُنفذ في سـياق هذه المنظومة الشـاملة. ويتجلى هذا التكامل في أن مخرجات التقييم تُغذي عمليات المعالجة، حيث تُحدد المخاطر ذات الأولوية التي تســتوجب تطوير ضـوابط وإجراءات، وتُسـتخدم كأسـاس لتصـميم برامج التدريب والتوعية، وتُوجه تخصــيص الميزانيات الأمنية، وتُســهم في تحديد متطلبات التأمين. كما أن عمليات المراقبة والمراجعة المسـتمرة تُغذي بدورها عمليات التقييم، من خلال توفير بيانات فعلية عن أداء الضــوابط وتغيرات بيئة المخاطر، مما يُمكن من تحديث تقديرات المخاطر وجعلها أكثر دقة مع مرور الوقت. ويشــمل التكامل أيضــاً ربط تقييم المخاطر الأمنية بتقييم المخاطر في المجالات الأخرى كالسـلامة والصـحة المهنية والبيئة والجودة، لتوفير صــورة شــاملة عن المخاطر التي تواجه المنشــأة وتجنب التعارض أو الازدواجية في جهود المعالجة. ويُوصــى بإنشــاء لجنة مركزية لإدارة المخاطر تضم ممثلين عن مختلف التخصصات، لتنسيق جهود التقييم والمعالجة عبر المجالات المختلفة، وضــمان اتســاق المنهجيات والمعايير، وتوفير رؤية شــاملة للإدارة العليا عن وضع المخاطر في المنشأة ككل."11"

وتُعد عملية تقييم مستوى المخاطر الأمنية بمثابة البوصلة التي توجه الجهود الأمنية في المنشـآت الحيوية، فهي تحول التحديد النوعي للمخاطر إلى أولويات قابلة للقياس والإدارة، وتمكن من اتخاذ قرارات مبنية على الأدلة بدلاً من الحدس أو التقديرات العشوائية. وعندما تُجرى هذه العملية بشكل منهجي ودقيق ومستمر، فإنها لا تحسن فقط فعالية الأمن، بل تُسـهم أيضـاً في تحسـين كفاءة اسـتخدام الموارد، وتعزيز ثقة الإدارة والعـاملين والجهـات الخـارجيـة في منظومـة الأمن، وتوفير أســاس متين للتحسين المستمر في مواجهة التهديدات المتطورة باستمرار."12"

اختبار الخطط والتمارين الأمنية

تمثل اختبارات الخطط والتمارين الأمنية الآلية العملية التي تنتقل فيها إدارة المخاطر من التنظير إلى التطبيق الملموس، حيث توفر بيئة محكومة لاختبار مدى فعالية السياسات والإجراءات والضوابط الأمنية في مواجهة سيناريوهات تهديدية معقولة. ويُعد هذا الركن من أركان إدارة المخاطر حلقة الوصل بين التخطيط والتنفيذ، إذ لا يمكن الجزم بفعالية أي خطة أمنية دون اختبارها في ظروف تحاكي الواقع بقدر كافٍ من الدقة، فهي الوسيلة التي تحول النصوص النظرية إلى قدرات عملية راسخة، وتُبني "الذاكرة العضلية" الاستجابة التي تمكن الفرق الأمنية من التصرف بكفاءة وهدوء تحت الضغط، تماماً كما تدرب الفرق العسكرية على سيناريوهات القتال قبل خوض المعارك الحقيقية."1"

أولاً: مفهوم التمارين الأمنية وأهميتها

تُعرف التمارين الأمنية بأنها عمليات محاكاة منظمة تُجرى لاختبار وتقييم وتحسين فعالية الخطط والإجراءات والأنظمة والكوادر الأمنية في مواجهة سيناريوهات تهديدية محددة. وتتجاوز أهميتها مجرد التحقق من سلامة الإجراءات، لتشمل بناء ثقافة أمنية تنظيمية، وتعزيز التنسيق بين الإدارات والجهات المختلفة، وتدريب الكوادر على اتخاذ القرارات تحت الضغط، وتحديد الفجوات والثغرات في الخطط قبل أن تستغلها التهديدات الحقيقية. وتُعد التمارين استثماراً استراتيجياً، إذ أن تكلفة اكتشاف الثغرات في بيئة تدريبية محكومة أقل بكثير من تكلفة اكتشافها في أثناء حادث أمني حقيقي، كما أنها تبني الثقة بين أعضاء الفرق الأمنية وتُرسخ قنوات الاتصال التي قد تكون شريان النجاة في الأزمات."2"

ثانياً: أنواع التمارين الأمنية

تتنوع التمارين الأمنية في المنشآت الحيوية وفقاً لأهدافها وتعقيدها وحجم المشاركة فيها، ويُمكن تصنيفها إلى ثلاثة مستويات رئيسية تتدرج في الواقعية والتعقيد. المستوى الأول هو **تمارين الطاولة(Tabletop Exercises)** ، وهي تمارين قائمة على المناقشة، تجمع المعنيين في غرفة واحدة لمناقشة سيناريو افتراضي

والتفكير في خطوات الاســـتجابة المطلوبة، دون أي تأثير فعلي على الأنظمة أو العمليات. تُستخدم هذه التمارين لاختبار الفهم المشترك للإجراءات، وتحديد الأدوار والمسؤوليات، وتقييم قنوات الاتصـال، وتُعد نقطة انطلاق ممتازة لأنها قليلة التكلفة وسهلة التنظيم، ولكنها تظل محدودة في قدرتها على اختبار الاستجابة العملية تحت الضغط."3"

المســـتوى الثاني هو **التمارين العملية المحدودة**، وتشـــمل محاكاة عملية لجزء من خطة الاســـتجابة، كتدريب فريق على التعامل مع إنذار حريق، أو اختبار نظام الإخلاء في مبنى معين، أو محاكاة هجوم سيبراني على نظام تشغيل محدد. تُستخدم هذه التمارين لاختبار عناصـــر محددة من الخطط، وتدريب الفرق على اســـتخدام المعدات والأدوات، وتقييم فعالية الإجراءات الفردية، وتكون أكثر واقعية من تمارين الطاولة ولكنها تظل محدودة النطاق.

أما المســـتوى الثالث والأكثر تعقيداً فهو **التمارين الشـــاملة واســـعة النطاق**، وهي تمارين تشـــمل جميع عناصـــر المنشـــأة أو أجزاء كبيرة منها، وتُجرى بالتعاون مع جهات خارجية، وقد تســـتمر أياماً وتشـــمل ســـيناريوهات متعددة الأبعاد. تُســـتخدم لاختبار التكامل بين جميع عناصر منظومة الأمن، والتنسيق مع الجهات الخارجية، وقدرة المنشـأة على الاستمرار في العمل أثناء الأزمات. وتُعد هذه التمارين الأقرب إلى الواقع والأكثر فائدة، ولكنها الأكثر تكلفة وتعقيداً في التنظيم."4"

ثالثاً: منهجية تصميم وتنفيذ التمارين الأمنية

تعتمد فعالية التمرين الأمني على جودة تصـــميمه ومنهجية تنفيذه، والتي تمر عادةً بمراحل متســـلســـلة تبدأ بتحديد الأهداف، وهي الخطوة الأكثر أهمية، حيث يجب أن تُحدد الأهداف بدقة ووضوح وتكون قابلة للقياس، كاختبار سرعة الاستجابة لحادث معين، أو تقييم فعالية قنوات الاتصال الداخلية، أو قياس دقة تنفيذ إجراءات الإخلاء. وتأتي بعدها مرحلة تصميم السيناريو، حيث يُبنى سيناريو واقعي ومركب يتناسب مع الأهداف المحددة وطبيعة التهديدات المحتملة، ويجب أن يكون السيناريو مفصلاً بما يكفي ليكون قابلاً للتنفيذ، ومرناً بما يسمح للمشاركين باتخاذ قرارات تؤثر على

مساره. وينبغي أن يتضمن السيناريو عناصر المفاجأة والتعقيد التي تميز الأحداث الحقيقية، كأن يقع حادث ثانوي أثناء التعامل مع الحادث الأول، أو أن تتعطل وسيلة اتصال أساسية في لحظة حساسة."5"

وتشمل مرحلة التخطيط للتمرين أيضاً تحديد المشاركين من مختلف الإدارات والجهات، وتوزيع الأدوار وتحديد المسؤوليات، وإعداد المواد اللازمة (كوصف السيناريو، وجداول الأحداث، وأدوات التقييم)، وتوفير الموارد المادية والبشرية، وتحديد جدول زمني واضح. ويُعد إشراك إدارة المنشأة في مرحلة التخطيط والتنسيق ضرورياً لضمان توفر الموارد والدعم اللازمين، كما يُوصى بالاستعانة بخبراء خارجيين في تصميم السيناريوهات المعقدة أو تقييم الأداء لضمان الموضوعية.

أما مرحلة التنفيذ فتشمل تقديم السيناريو للمشاركين، وتيسير سير التمرين، وإدارة "الإيقاعات (Injects) "وهي الأحداث التي تُضاف خلال التمرين لتغيير مساره أو إضافة تعقيدات، ومراقبة أداء المشاركين وتوثيق القرارات والإجراءات التي يتخذونها. وتُستخدم فرق تقييم مستقلة في التمارين الكبيرة لمراقبة الأداء الموضوعي دون التأثير على سير التمرين. وتُختتم عملية التمرين بمرحلة ما بعد التنفيذ، وتشمل جلسة نقدية فورية للمشاركين لتبادل الانطباعات الأولية، وإعداد تقرير تقييم مفصل يتضمن نقاط القوة والضعف والتوصيات، ووضع خطة لمعالجة الثغرات المكتشفة، ومتابعة تنفيذ التوصيات."6"

رابعاً: أنواع السيناريوهات والتهديدات التي تُختبر

تتنوع السيناريوهات التي تُستخدم في التمارين الأمنية لتعكس طبيعة التهديدات المحتملة التي قد تواجه المنشأة، وتشمل الهجمات السيبرانية بأنواعها، كاختراق أنظمة التحكم الصناعية، وهجمات برامج الفدية، وهجمات حجب الخدمة، والتصيد الإلكتروني الذي يستهدف العاملين. وتشمل أيضاً السيناريوهات المادية كحوادث الاقتحام والتسلل، والهجمات المسلحة، والتفجيرات، وعمليات التخريب، وسرقة المواد أو المعلومات الحساسة. ولا تغفل السيناريوهات حالات الطوارئ غير

المتعمدة، كالحرائق الكبيرة، والتسـريبات الكيميائية أو الإشـعاعية، والكوارث الطبيعية كالزلازل والفيضـانات، والأزمات الصـحية كتفشـي الأمراض المعدية التي قد تعطل حضور العاملين. ويُستخدم في التمارين المتقدمة سيناريوهات مركبة تجمع بين عدة تهديدات في وقت واحد، كهجوم سـيبراني يتبعه اقتحام مادي، أو حادث طبيعي يعقبه أزمة في سلاسل التوريد. ويُوصـى بتنويع السيناريوهات لتشمل أيضـاً الحالات الأقل احتمالاً ولكن الأعلى تأثيراً، كالهجمات الإرهابية واسـعة النطاق أو الكوارث الطبيعية النادرة، لأن المفاجأة في هذه الحالات قد تكون أكبر ودرجة الاستعداد لها أقل."7"

خامساً: المشاركون وأدوارهم في التمارين الأمنية

تتطلب التمارين الأمنية الفعالة مشـاركة مجموعة متنوعة من الأدوار، تتجاوز بكثير الفريق الأمني المباشـر. وتشـمل هذه الأدوار فريق الدفاع (الفريق الأزرق) المكلف بالاسـتجابة للتهديد وتنفيذ الإجراءات الأمنية وحماية الأصـول، والذي يضـم عادةً أفراد الأمن والكوادر التقنية ومسـؤولي العمليات. ويُقابلهم فريق الهجوم (الفريق الأحمر) المكلف بمحاكاة التهديد ومحاولة اختراق الدفاعات، ويتكون عادةً من خبراء داخليين أو خارجيين في مجال التهديدات المعنية (كخبراء الأمن السـيبراني أو المحققين). ويُضـاف إليهم فريق التقييم (الفريق الأبيض) المكلف بمراقبة أداء الفرقين، وتقييم الاستجابة، وتوثيق الدروس المستفادة، ويُفضل أن يكون هذا الفريق محايداً ومستقلاً عن الفرق المشاركة لضمان موضوعية التقييم.

وتشـمل الأدوار الأخرى الإدارة العليا الممثلة في صـناع القرار الاسـتراتيجي، والإدارات الداعمة كالشؤون القانونية والعلاقات العامة والموارد البشرية، والجهات الخارجية كالشـرطة والدفاع المدني والجهات الحكومية المنظمة والشـركاء. وتزداد أهمية مشـاركة الإدارة العليا في التمارين، لأن القرارات الحاسـمة في الأزمات الحقيقية غالباً ما تتطلب موافقتهم أو توجيههم، وغيابهم عن التمرين يترك فراغاً في محاكاة الواقع ويُقلل من التزامهم بتنفيذ التوصـيات. وقد أظهرت تجارب المنشـآت

التي أجرت تمارين شـاملة أن نجاح التمرين يرتبط بشـكل كبير بمسـتوى مشـاركة الإدارة العليا والتزامها بتطبيق الدروس المستفادة."8"

سادساً: تقييم التمارين واستخلاص الدروس

لا تكتمل قيمة التمرين الأمني دون عملية تقييم منهجية تستخلص الدروس وتُترجمها إلى تحسـينات ملموسـة. وتشـمل عملية التقييم جمع البيانات من مصـادر متعددة، كـالملاحظـة المبـاشـرة من فريق التقييم، وسـجلات القرارات والإجراءات خلال التمرين، وشـهادات المشـاركين وآرائهم، ومقارنة الأداء الفعلي بالأداء المخطط له في الخطة. ويُسـتخدم تحليل الفجوات لتحديد مواطن الضـعف والثغرات في الخطط أو الإجراءات أو التدريب أو الأنظمة، وتحليل الأسـباب الجذرية لفهم لماذا حدثت هذه الفجوات، وليس فقط وصفها.

وتُنتج عملية التقييم قائمة محددة ومرتبة حسـب الأولوية بالتوصـيات والإجراءات التصـحيحية، مع تحديد مسـؤول التنفيذ والجدول الزمني والميزانية المطلوبة. ويُوصى بإعداد تقرير تقييم شامل يُوزع على جميع المعنيين، وعقد جلسة استعراض نهائية مع المشـاركين والإدارة لمناقشـة النتائج والتوصـيات. ويُعد متابعة تنفيذ التوصيات من أهم مراحل التمرين، إذ أن إهمالها يعني أن التمرين كان مجرد نشاط شكل غير مثمر، وتُستخدم نتائج التقييم لتحديث الخطط الأمنية، وتعديل الإجراءات، وتحسين برامج التدريب، وإجراء تغييرات تنظيمية أو تقنية عند الحاجة."9"

سابعاً: التمارين المشتركة والتنسيق مع الجهات الخارجية

تتطلب طبيعة التهديدات التي تواجه المنشـآت الحيوية تعاوناً وثيقاً مع جهات متعددة خارج المنشـأة، مما يسـتوجب إجراء تمارين مشـتركة تجمع هذه الأطراف وتختبر قنوات التنسـيق فيما بينها. وتشـمل هذه التمارين الشـراكات مع الأجهزة الأمنية كالشـرطة والاسـتخبارات، ووكالات الطوارئ كالدفاع المدني والإسـعاف، والجهات التنظيمية والحكومية، والمنشآت المجاورة أو الشريكة التي تشترك في نفس شبكات البنية التحتية، ومقدمي الخدمات والموردين الذين يعتمد عليهم استمرار العمل.

وتُعد التمارين المشـتركة فرصـة لا تعوض لبناء الثقة والعلاقات الشـخصـية بين الأفراد الذين سـيعملون معاً في حالات الطوارئ الحقيقية، واختبار مدى توافق الإجراءات والبروتوكولات بين الأطراف المختلفة، وتحديد نقاط الاحتكاك أو الثغرات في التنسيق قبل أن تتسبب في أزمات حقيقية. وقد أظهرت تجارب التمارين المشـتركة في العديد من الدول أن بناء علاقات عمل وثيقة بين القطاعين العام والخاص، عبر تمارين أمنية منتظمة، يُعزز الاستجابة الجماعية للأزمات ويُسهم في تقليل زمن الاستجابة وتحسين جودة القرارات المتخذة في الأوقات الحرجة."10"

ثامناً: دور التكنولوجيا في التمارين الأمنية

شهدت التمارين الأمنية تطوراً كبيراً بفضل التقدم التكنولوجي، إذ أصبحت تستخدم منصـات محاكاة متطورة تتيح خلق بيئات تدريبية واقعية دون تعريض الأنظمة الحقيقية للخطر. وتشـمل هذه المنصـات "ميدان التدريب السـيبراني (Cyber Range)" الذي يحاكي الشبكات والأنظمة الحقيقية في بيئة معزولة، ويسمح بتدريب الفرق على مواجهة هجمات سـيبرانية معقدة بأمان تام. وتُسـتخدم أيضـاً نماذج مصغرة مادية للبنية التحتية، كالمحطات البحرية ومحطات معالجة المياه المصغرة، التي تسمح باختبار تأثير الهجمات السيبرانية على العمليات المادية في بيئة خاضعة للرقابة. وتُستخدم تقنيات الذكاء الاصطناعي لتوليد سيناريوهات تدريبية أكثر تعقيداً وتنوعاً، ولتحليل أداء المشـاركين وتقديم تغذية راجعة فورية. وتُمكّن التكنولوجيا أيضـاً من إجراء تمارين عن بُعد بمشـاركة فرق من مواقع جغرافية متعددة، مما يُسهل التمارين المشتركة عبر المنشآت والقطاعات والدول. ويُوصى بالاستثمار في هذه التقنيات بما يتناسـب مع حجم المنشـأة وتعقيدها وميزانيتها، والاسـتفادة من المنصات والمرافق المتاحة عبر الجهات الحكومية أو الأكاديمية عند الإمكان."11"

تاسعاً: التحديات والعوائق في تنفيذ التمارين الأمنية

تواجه المنشـآت الحيوية مجموعة من التحديات التي قد تعيق تنفيذ التمارين الأمنية بفعالية، ويجب التخطيط لتجاوزها مسبقاً. ومن أبرز هذه التحديات محدودية الموارد المالية والبشرية، حيث تُعتبر التمارين الواسعة مكلفة وتستهلك وقتاً وجهداً كبيرين،

وقد تُواجه صـــعوبة في تبرير هذه التكاليف أمام الإدارة العليا في أوقات الاســتقرار الأمني النسـبي. ويُمثل نقص الخبرة في تصـميم وإدارة التمارين تحدياً آخر، خاصـة في المنشآت المتوسطة التي قد لا تتوفر فيها كوادر متخصصـة في هذا المجال، مما قد يؤدي إلى تمـارين غير واقعيـة أو غير مفيـدة. كمـا قد تُواجـه التمـارين مقـاومـة تنظيمية من بعض الإدارات التي ترى فيها عبئاً إضـافياً أو تهديداً لصـورتها، خاصـة إذا كانت التمارين تكشف عن تقصير أو قصور في أدائها. ويُضاف إلى ذلك صعوبة تصـــميم ســـيناريوهات واقعية ومركبة بما يكفي لتكون مفيدة، دون أن تكون معقدة للغاية بحيث تفقد المشـــاركين القدرة على التفاعل معها، إضـــافة إلى التحدي الأكبر المتمثل في تحويل نتائج التمارين إلى تحسـينات فعلية، وعدم ترك التوصـيات حبراً على ورق بعد انتهاء التمرين. وللتغلب على هذه التحديات، يُوصـــى بتدرج التمارين من البســـيطة إلى المعقدة، والاســـتفادة من خبرات خارجية عند الحاجة، وإشـــراك الإدارة العليا في التخطيط والتنفيذ لضـــمان التزامها، وإبراز النجاحات والدروس المســـتفادة كدليل على قيمة التمارين، وجعل التمارين جزءاً من الثقافة التنظيمية وليس نشاطاً استثنائياً."12"

آليات الوقاية والسيطرة على المخاطر

تمثل آليات الوقاية والسيطرة على المخاطر الجسر الذي ينقل مخرجات تقييم المخاطر من التحليل النظري إلى الإجراءات العملية، فهي الأدوات والوسائل والإجراءات التي تُتخذ لمنع المخاطر من التحقق، أو لتقليل تأثيرها إذا وقعت، أو للسيطرة عليها ومنع انتشارها. وتقوم فلسفة هذه الآليات على مبدأ أن الأمن الفعال لا يقتصر على وضع الخطط، بل يمتد إلى تنفيذها وتطبيقها على أرض الواقع، مع القدرة على التكيف والاستجابة السريعة عند حدوث أي طارئ. وتتنوع آليات الوقاية والسيطرة بين المادية والتقنية والبشرية والإجرائية، وتتكامل فيما بينها لتشكل منظومة دفاعية متعددة الطبقات، تبدأ بإجراءات الوقاية التي تمنع الخطر من الحدوث، وتستمر بآليات الكشف المبكر التي تكتشفه في مهدها، ثم إجراءات الاحتواء التي تمنع انتشاره، وأخيراً إجراءات التعافي التي تعيد الأمور إلى طبيعتها بعد السيطرة عليه."1"

أولاً: آليات الوقاية من المخاطر (المنع)

تُعد آليات الوقاية (أو المنع) المستوى الأول والأكثر أهمية في السيطرة على المخاطر، فهي تهدف إلى منع الخطر من التحقق أساساً، وبالتالي تجنب الحاجة إلى التعامل مع عواقبه. وتتنوع آليات الوقاية لتشمل مجموعة واسعة من الإجراءات التي تُطبّق في مراحل التخطيط والتصميم والتشغيل اليومي للمنشأة. وتشمل هذه الآليات التصميم الأمني المتكامل للمنشأة منذ مرحلة التخطيط (Security by Design)، بحيث تُدمج الاعتبارات الأمنية في التصميم الهندسي والمعماري قبل البناء، كاختيار مواقع المداخل وتوزيع المرافق وتصميم الممرات بما يقلل من نقاط الضعف المحتملة. وتشمل أيضاً تطبيق سياسات وإجراءات أمنية مكتوبة وموثقة تُحدد بوضوح مسؤوليات وصلاحيات الأفراد وآليات التعامل مع المخاطر، وتوعية وتدريب العاملين على السلوكيات الآمنة، وتطبيق نظام صارم للتحقق من الهوية والصلاحيات قبل منح الدخول إلى المناطق الحساسة، واستخدام الحواجز المادية والأسوار والبوابات التي تمنع الوصول غير المصرح به، وتطبيق إجراءات التفتيش

المنتظمة للأفراد والمركبات والبضـــائع، وتحديث الأنظمة التقنية (كالبرمجيات وأجهزة الأمن) باستمرار لسد الثغرات المكتشفة، وبناء علاقات مع الأجهزة الأمنية للحصول على المعلومات الاستباقية عن التهديدات المحتملة."2"

ثانياً: آليات الكشف المبكر والإنذار

على الرغم من فعالية آليات الوقاية، لا يمكن ضـــمان منع جميع المخاطر، مما يستوجب وجود آليات للكشف المبكر تتيح اكتشاف الخطر في مراحله الأولى قبل أن يتطور إلى حادث كبير. وتشـمل هذه الآليات أنظمة المراقبة المسـتمرة كالكاميرات الحرارية والنهارية وأجهزة اسـتشـعار الحركة والاهتزاز، وأنظمة كشـف الغازات والمواد الكيميائية والإشـعاعية المنتشـرة في محيط المنشـأة، وأنظمة كشـف التسـلل المحيطية المثبتة على الأسوار وفي التربة، وأنظمة كشف الاختراق السيبراني التي تراقب حركة البيانات وتنبّه إلى أي نشـاط غير طبيعي، وأجهزة الإنذار اليدوية التي تسـمح للعاملين بالإبلاغ عن أي ملاحظات مشـبوهة، وأنظمة التحليل الذكي للفيديو التي تكشـف السـلوكيات الشـاذة تلقائياً. وتتصـل هذه الأنظمة بغرفة تحكم مركزية تتلقى التنبيهات وتصنفها وفق درجة الخطورة، وتُفعّل إجراءات الاستجابة المناسبة، وتُسـجل البيانات للاستفادة منها في التحليل والتحسين المستقبليين. ويُعد الربط بين أنظمة الكشـف والإنذار أمراً حيوياً، إذ تنتقل المعلومة تلقائياً من جهاز الكشـف إلى نظام الإنذار الذي يُعلم الفرق المختصـة فوراً، مما يُقلل زمن الاسـتجابة بشـكل كبير ويمنح المنشأة فرصة حاسمة للتصرف قبل تفاقم الأزمة."3"

ثالثاً: آليات احتواء المخاطر والاستجابة السريعة

عندما يقع الخطر رغم إجراءات الوقاية والكشـف، تأتي آليات الاحتواء والاسـتجابة السريعة للحد من انتشاره وتقليل آثاره، وتشكل خط الدفاع الثاني بعد الوقاية. وتشمل هذه الآليات تفعيل خطط الطوارئ المُعدة مسـبقاً، والتي تُحدد الإجراءات الواجب اتخاذها في كل سيناريو، وتوزيع الأدوار والمسؤوليات بوضوح، وقنوات الاتصال المحددة مسبقاً لضمان سرعة التبليغ. وتشمل أيضاً إجراءات العزل السريع للمناطق المتضـررة لمنع انتشـار الخطر (كإطفاء الحريق ومنع انتشـاره، أو عزل التسـرب

الكيميائي، أو قطع الشبكة المخترقة لمنع انتشار الاختراق)، وتفعيل أنظمة الإغلاق والفتح الآلي للأبواب لتوجيه الحركة ومنع التسلل، وتفعيل فرق الاستجابة المتخصصة المدربة على التعامل مع مختلف أنواع الحوادث، وتفعيل أنظمة الاتصال الطارئ مع الجهات الخارجية كالدفاع المدني والإسعاف والشرطة، وإخلاء المناطق المتضررة وحماية الأفراد من الخطر. وتُعد سرعة الاستجابة عاملاً حاسماً في نجاح الاحتواء، فكلما كانت الاستجابة أسرع، قلّ حجم الأضرار وانتشار الخطر، وزادت فرصة السيطرة عليه قبل أن يتفاقم. ولذلك، تُجرى تدريبات دورية لفرق الاستجابة لضمان جاهزيتها وقدرتها على التصرف بسرعة وفعالية تحت الضغط."4"

رابعاً: آليات التعافي واستمرارية العمل

بعد السيطرة على الخطر واحتوائه، تأتي مرحلة التعافي التي تهدف إلى إعادة المنشأة إلى حالتها الطبيعية في أقصر وقت ممكن، مع ضمان استمرارية الوظائف الحيوية خلال فترة التعافي. وتشمل آليات التعافي خطط استمرارية العمل (Business Continuity Plans)التي تُحدد كيفية استمرار العمليات الحيوية خلال الأزمة وبعدها، بما في ذلك تحديد الوظائف الأساسية التي يجب أن تستمر بأي ثمن، وتوفير أنظمة ومعدات بديلة، وتحديد الموردين البديلين، وتوزيع المهام على فرق بديلة في حال غياب الفرق الأساسية. وتشمل أيضاً خطط التعافي من الكوارث (Disaster Recovery Plans) التي تُحدد كيفية استعادة الأنظمة والبيانات والعمليات بعد توقفها، كاستعادة النسخ الاحتياطية للبيانات، وإعادة تشغيل الأنظمة تدريجياً، وإصلاح الأضرار المادية في المباني والمعدات. ويُعد التقييم بعد الحادث (Post-Incident Review) جزءاً أساسياً من التعافي، إذ يُحلل الحادث لتحديد الدروس المستفادة، وتقييم فعالية الاستجابة، وتحديث الخطط والإجراءات بناءً على الخبرات المكتسبة، مما يحسّن مناعة المنشأة ضد حوادث مستقبلية مماثلة. ويُوصى بأن تكون خطط التعافي جزءاً مدمجاً في ثقافة المنشأة، وأن تُختبر وتُحدث بشكل دوري لضمان بقائها عملية وفعالة."5"

خامساً: الضوابط المادية للوقاية من المخاطر

تُعد الضـوابط المادية من أقدم وأكثر آليات الوقاية انتشـاراً، وتشـمل جميع العناصـر الملموسة التي تُستخدم لمنع أو تأخير الوصول غير المصرح به إلى أصول المنشأة. وتشـمل هذه الضـوابط الأسـوار والحواجز التي تحيط بالمنشـأة وتمنع الاقتراب غير المصرح به، وتتنوع بين الخرسانية والمعدنية والكهربائية والإلكترونية، مع مراعاة الارتفاع والمتانة وعدم وجود نقاط عمياء. وتشـــمل الأقفال والبوابات بأنواعها المختلفة، من الميكانيكية البسـيطة إلى الإلكترونية والبيومترية المتطورة، التي تُغلق المداخل والمخارج وتحد من الدخول. وتشـمل أنظمة الإضـاءة الأمنية التي تضـيء المحيط والمناطق الحيوية، وتزيل الظلام الذي قد يسـتغله المتسـللون. وتشـمل الحواجز المانعة لاقتحام المركبات كالأعمدة القابلة للرفع والحواجز الخرسانية، التي تمنع المركبات من اختراق المحيط بسـرعة عالية. وتشـمل أيضـاً الزجاج المصـفح والمقاوم للكسر في النوافذ والأبواب، والجدران المقاومة للرصاص والانفجارات في المناطق الحيوية، والأبواب المدرعة. وتُصـمم هذه الضـوابط المادية وفق مبدأ الدفاع المتعمق، بحيث تُوضـع طبقات متعددة من الحماية، كلما اخترقت طبقة، واجه المهاجم طبقة أخرى أكثر صرامة، مما يمنح الوقت الكافي للاستجابة الأمنية."6"

سادساً: الضوابط التقنية للوقاية من المخاطر

مع تزايد الاعتماد على التقنية في المنشآت الحيوية، أصبحت الضوابط التقنية تشكل جزءاً متزايد الأهمية في آليات الوقاية والسـيطرة على المخاطر. وتشـمل هذه الضـوابط أنظمة التحكم بالدخول الإلكترونية التي تعتمد على البطاقات الذكية أو القياسات الحيوية، وتُسجل كل عملية دخول وخروج وتمنع الوصول غير المصرح به. وتشـمل أنظمة المراقبة بالفيديو الذكية التي تُغطي المحيط والمناطق الداخلية، وتُحلل الصور للكشف عن السلوكيات المشبوهة تلقائياً. وتشمل أنظمة كشف التسلل الإلكترونية كأجهزة استشعار الحركة والاهتزاز والأشعة تحت الحمراء، التي تنبه إلى أي حركة غير مصـرح بها. وفي الجانب السـيبراني، تشـمل جدران الحماية وأنظمة كشـف ومنع الاختراق، التي تحمي الشـبكات والأنظمة من الهجمات

الإلكترونية، وأنظمة التشفير القوي التي تحمي البيانات أثناء التخزين والنقل، وأنظمة المصادقة متعددة العوامل التي تجعل اختراق الحسابات أمراً بالغ الصعوبة، وأنظمة إدارة الثغرات التي تكتشف وتعالج نقاط الضعف في البرمجيات قبل أن يستغلها المهاجمون. ويُعد التكامل بين هذه الضوابط التقنية والضوابط المادية والبشرية عنصراً حاسماً في فاعليتها، إذ لا يمكن لأي ضابط منفرد أن يوفر حماية كافية."7"

سابعاً: الضوابط البشرية للوقاية من المخاطر

يُعد العنصر البشري من أهم عناصر المنظومة الأمنية، وفي الوقت نفسه من أكثرها عرضة للخطأ والاستغلال، مما يجعل الضوابط البشرية ركيزة أساسية في الوقاية من المخاطر. وتشمل هذه الضوابط التدريب والتوعية الأمنية المستمرة لجميع العاملين، لضمان فهمهم للمخاطر وإجراءات التعامل معها، وتحويلهم من مجرد مستخدمين للأنظمة إلى شركاء فاعلين في الحماية. وتشمل برامج التوعية تعريف العاملين بالتهديدات الحالية (كالتصيد الإلكتروني والهندسة الاجتماعية)، وتدريبهم على كيفية التعرف عليها والإبلاغ عنها، وتعزيز السلوكيات الآمنة كاستخدام كلمات مرور قوية وعدم مشاركتها، وقفل الأجهزة عند المغادرة، والإبلاغ عن أي نشاط مشبوه. وتشمل الضوابط البشرية أيضاً إجراءات التوظيف الآمن، كالتحقق من الخلفيات الأمنية للموظفين الجدد، والتأكد من أهليتهم للعمل في المناصب الحساسة، وإجراء مقابلات أمنية عند الحاجة. وتشمل تطبيق سياسات الفصل بين الصلاحيات، بحيث لا يتمتع أي فرد بصلاحيات واسعة بمفرده، مما يقلل من خطر سوء الاستخدام. وتشمل أيضاً خطط التناوب والإجازات الإجبارية للمناصب الحساسة، لكشف أي مخالفات أو تجاوزات قد تحدث، وتوفير قنوات آمنة للإبلاغ عن المخالفات الأمنية دون خوف من الانتقام. ويُعد الاستثمار في العنصر البشري أحد أكثر الاستثمارات الأمنية جدوى، إذ أن عاملاً مدرَّباً وواعياً يمكن أن يمنع حوادث كانت ستكلّف المنشأة مبالغ طائلة."8"

ثامناً: الضوابط الإجرائية والتنظيمية للوقاية من المخاطر

تُمثل الضـوابط الإجرائية والتنظيمية الإطار الذي ينظم عمل جميع العناصـر الأمنية الأخرى، وتضـمن اتسـاقها وفعاليتها واسـتمراريتها. وتشـمل هذه الضـوابط وضـع سياسـات أمنية مكتوبة وموثقة تغطي كافة جوانب الأمن في المنشـأة، وتُحدث بشكل دوري لمواكبة التغيرات، مع تحديد مسـؤوليات وواجبات كل فرد وإدارة بشـكل واضـح. وتشـمل وضـع إجراءات تشـغيلية موحدة (SOPs) لكل مهمة أمنية، تُحدد الخطوات الواجب اتباعها بدقة، وتوفر مرجعاً موثوقاً للعاملين وتضـمن الاتسـاق في الأداء. وتشـمل آليات الرقابة والتدقيق الداخلي، كالتفتيش الدوري والتقييم الذاتي، والتدقيق الخارجي من جهات مسـتقلة، والتي تكشـف الثغرات قبل أن يسـتغلها المهاجمون. وتشـمل خطط الطوارئ واسـتمرارية العمل، التي تُعد مسـبقاً وتُختبر دورياً، لتكون جاهزة للتفعيل عند الحاجة. وتشمل إدارة التغيير الأمني، التي تضـمن أن أي تغيير في الأنظمـة أو الإجراءات أو الهيكـل التنظيمي يُراجع من النـاحيـة الأمنية قبل تنفيذه. وتشمل أيضاً آليات الإبلاغ عن الحوادث الأمنية وتحليلها، لضمان التعلم من الأخطاء ومنع تكرارها، ونظام إدارة الوثائق الأمنية الذي يضـمن توفر المعلومات الصـحيحة للمعنيين عند الحاجة، وحماية هذه الوثائق من الوصـول غير المصرح به."9"

تاسعاً: التكامل بين آليات الوقاية والسيطرة

لا يمكن لأي آلية منفردة أن توفر حماية كافية للمنشـآت الحيوية، بل تتحقق الفعالية القصوى من خلال التكامل العضوي بين جميع آليات الوقاية والسيطرة، بحيث تشكل منظومة دفاعية متعددة الطبقات تُعرف بمبدأ "الدفاع المتعمق (Defense in Depth)". ويعني هذا المبدأ أن تُوضـع طبقات متعددة من الحماية، كل منها يعتمد على آليات مختلفة، بحيث إذا اخترقت إحدى الطبقات، تظل الطبقات الأخرى قادرة على منع أو احتواء الخطر. فمثلاً، يُمكن أن يجمع نظام أمن المنشـأة بين السـياج الخارجي (ضـابط مادي)، وكاميرات المراقبة (ضـابط تقني)، ودوريات الأمن (ضابط بشري)، وسياسات الدخول الصارمة (ضابط إجرائي)، بحيث لا يعتمد أمن

المنشأة على أي عنصر بمفرده. ويُحقّق هذا التكامل أيضاً تنويعاً في نقاط القوة، فما قد يفشل فيه الضابط المادي قد تنجح فيه التقني، وما قد يخطئ فيه البشري قد تصححه الإجرائي. ويُوصى بتصميم المنظومة الأمنية بحيث تتداخل هذه الآليات وتدعم بعضها البعض، وتُختبر بشكل دوري للتأكد من استمرار تكاملها وفعاليتها. وقد أظهرت الدراسات أن المنشآت التي تتبنى نهجاً تكاملياً في وقاية وسيطرة المخاطر تحقق مستويات أمان أعلى بتكاليف إجمالية أقل، مقارنة بتلك التي تعتمد على آليات منفردة أو غير متكاملة."10"

عاشراً: التحديث المستمر لآليات الوقاية والسيطرة

تتسم بيئة التهديدات التي تواجه المنشآت الحيوية بالتطور المستمر، سواء من حيث ظهور تهديدات جديدة، أو تطوّر أساليب ووسائل التهديدات القائمة، مما يستوجب تحديثاً مستمراً لآليات الوقاية والسيطرة لمواكبة هذه التغيرات. ويتطلب هذا التحديث مراقبة مستمرة لتطورات بيئة التهديدات من خلال متابعة التقارير الاستخبارية والأمنية، وتحليل الحوادث التي وقعت في منشآت مماثلة، والاشتراك في منتديات ومراكز تبادل المعلومات الأمنية. كما يتطلب متابعة التطورات التكنولوجية وتقييم إمكانية تطبيقها في تحسين الأمن، كتقنيات الذكاء الاصطناعي في تحليل الفيديو، وتقنيات البلوكتشين في توثيق البيانات، وتقنيات الكشف الكمي في الأمن السيبراني. ويشمل التحديث أيضاً إعادة تقييم المخاطر بشكل دوري، لتعكس التغيرات في الأصول أو العمليات أو البيئة الخارجية، ومراجعة فعالية الضوابط الحالية وتعديلها أو استبدالها عند اللزوم، وتحديث سياسات وإجراءات الأمن لتتناسب مع المتغيرات الجديدة، وتدريب الكوادر على المهارات والمعارف الجديدة. وتُعد عملية التحديث المستمر استثماراً في المستقبل، إذ تحافظ على قدرة المنشأة على مواجهة التهديدات الجديدة والمتطورة، وتمنع تقادم المنظومة الأمنية الذي قد يجعلها عرضة للاختراق رغم الجهود السابقة المبذولة في بنائها."11"

وتُشكل آليات الوقاية والسيطرة على المخاطر العمود الفقري لمنظومة الأمن في المنشآت الحيوية، إذ تحول المعرفة النظرية بالمخاطر إلى قدرات عملية تحمي

الأصــول وتضــمن اســتمرارية العمليات. وتتطلب هذه الآليات التزاماً مســتمراً من جميع المســـتويـات التنظيميـة، بـدءاً من الإدارة العليـا التي تُوفر الموارد وتُحـدد السياسات، وصـولاً إلى كل عامل يطبّق الإجراءات اليومية ويسـهم في تعزيز الثقافة الأمنية. وعندما تُصــمم وتُنفذ هذه الآليات بشــكل متكامل ومســتدام، فإنها لا تقلل من المخاطر فحســب، بل تبني مرونة تنظيمية تمكن المنشــأة من التكيف مع الصــدمات والتعافي منها بسرعة، مما يُعزز قدرتها التنافسية وسمعتها واستقرارها على المدى الطويل."12"

غرفة عمليات إدارة الأزمات

تمثل غرفة عمليات إدارة الأزمات - (Emergency Operations Center EOC) القلب النابض لمنظومة إدارة المخاطر الأمنية في المنشآت الحيوية، إذ تُعد المركز العصبي الذي تتجمع فيه جميع خيوط المعلومات، وتُتخذ فيه القرارات الحاسمة، وتُنسق منه الجهود بين جميع الجهات المعنية لإدارة الأزمة والسيطرة عليها. وتختلف غرفة العمليات عن غرف التحكم التقليدية في كونها ليست مجرد موقع لمراقبة الأنظمة، بل هي بيئة متكاملة لإدارة الأزمات على المستوى الاستراتيجي والتكتيكي، تجمع بين القدرات التقنية والتنظيمية والبشرية لضمان استمرارية الاستجابة الفعالة في أصعب الظروف .ويُعد تصميم وتجهيز وتشغيل غرفة العمليات استثماراً استراتيجياً يُترجم الالتزام بإدارة المخاطر إلى قدرات عملية، ويُحدد غالباً الفارق بين أزمة يتم احتواؤها بسرعة وأخرى تتطور إلى كارثة .

أولاً: مفهوم غرفة عمليات إدارة الأزمات ووظائفها الأساسية

تُعرّف غرفة عمليات إدارة الأزمات بأنها المقر المخصص والمعزز تقنياً وتنظيمياً الذي يضم كبار المسؤولين والخبراء من مختلف الإدارات والجهات، ويعمل كمركز قيادة وتنسيق لإدارة الاستجابة للطوارئ والأزمات. وتتجاوز وظيفتها مجرد استقبال البلاغات، لتشمل جمع وتحليل المعلومات الواردة من جميع المصادر الداخلية والخارجية، وتقييم الموقف وتحديث تقديرات المخاطر بشكل لحظي، واتخاذ القرارات الاستراتيجية والتكتيكية وتوجيه الفرق الميدانية، وتنسيق جهود جميع الإدارات والجهات المشاركة في الاستجابة، وضمان استمرارية قنوات الاتصال مع كافة المعنيين، وإدارة العلاقات مع وسائل الإعلام والجمهور، وتوثيق كافة الإجراءات والقرارات للاستفادة منها في المراجعات المستقبلية. وتؤدي غرفة العمليات دوراً محورياً في تحويل الفوضى المحتملة إلى استجابة منظمة، وفي ضمان أن القرارات تُتخذ في الوقت المناسب وبمعلومات دقيقة، مما يُقلل من تأثير الأزمة ويسرع من التعافي .

ثانياً: التصميم الهندسي والتجهيزات التقنية لغرفة العمليات

يُعد التصـميم الهندسـي لغرفة عمليات إدارة الأزمات عاملاً حاسـماً في فعاليتها، إذ يجب أن يُصـمم المقر ليتحمل الظروف القاسـية ويسـتمر في العمل رغم تعطل الأنظمة والمرافق المحيطة. ويشمل التصميم اختيار موقع استراتيجي آمن، غالباً ما يكون محصـناً ومحمياً من التهديدات المادية والطبيعية، مع مراعاة سـهولة الوصـول إليه للمعنيين. وتُجهز غرفة العمليات بأنظمة طاقة احتياطية متعددة المسـتويات)كأنظمة N+1 أو ٢ Nلضـمان عدم انقطاع الطاقة أبداً (، وأنظمة تبريد وتكييف مستقلة، وأنظمة اتصالات متعددة ومتنوعة (أرضية، لاسلكية، فضائية) لضمان عدم انقطاع التواصل، وشبكات اتصال مؤمنة ومشفرة لنقل البيانات الحساسة، وشاشات عرض كبيرة تفاعلية تُتيح عرض المعلومات من مصـادر متعددة، وأنظمة معلومات وإدارة بيانات متطورة تعمل في الوقت الفعلي، وأنظمة أمن مادي وإلكتروني مشددة لحماية الغرفة نفسها ومن فيها. وتُصمم الغرفة عادةً لتستوعب فرق العمل الموسعة في حالات الأزمات الكبرى، وتُقسّـم إلى مناطق وظيفية كمنطقة القيادة، ومنطقة التحليل المعلوماتي، ومنطقة الاتصالات والإعلام، ومنطقة دعم القرار .

ثالثاً: الهيكل التنظيمي وأدوار الكوادر في غرفة العمليات

لا يمكن للتجهيزات التقنية وحدها أن تضـمن نجاح غرفة العمليات، بل تحتاج إلى هيكل تنظيمي واضـح وكوادر مدربة على أعلى مسـتوى. ويُحدد الهيكل التنظيمي عادةً قائد الأزمة (غالباً مدير المنشأة أو من يفوضه)، الذي يتحمل المسؤولية النهائية عن جميع القرارات ويتولى التنسـيق مع أعلى المسـتويات. ويعاونه مدير العمليات (أو رئيس غرفة العمليات) الذي يدير سـير العمل اليومي داخل الغرفة ويُنسـق بين الفرق، وفريق المعلومات والتحليل الذي يجمع المعلومات ويحللها ويُعد التقارير للمسؤولين، وفريق التخطيط الذي يُطور خيارات الاستجابة ويُعد الخطط التكتيكية، وفريق الاتصـالات والإعلام الذي يدير التواصـل الداخلي والخارجي والعلاقات الإعلامية، وفريق الدعم اللوجسـتي الذي يوفر الموارد والمعدات المطلوبة للاسـتجابة. وتُحدد الأدوار والمسـؤوليات بدقة في وثائق خطط الطوارئ، وتُختبر

وتُمارس بشكل دوري في التمارين الأمنية، لضمان أن الجميع يعرف دوره ويتقنه قبل وقوع الأزمة الحقيقية .

رابعاً: عمليات غرفة العمليات أثناء الأزمات

تُفعّل غرفة عمليات إدارة الأزمات وفق مستويات متدرجة تتناسب مع حجم الأزمة ودرجة خطورتها، وتتراوح بين المستوى الأدنى الذي يُقتصر فيه على المراقبة والاستعداد، والمستوى الأقصى الذي يُعبأ فيه كامل الموارد وتُستدعى جميع الجهات. وتتضمن العمليات النموذجية لغرفة العمليات أثناء الأزمة تنشيط الغرفة واستدعاء الفرق حسب المستوى المطلوب، وجمع المعلومات من المصادر الداخلية (كاميرات، أجهزة استشعار، تقارير ميدانية) والخارجية (جهات حكومية، استخبارات، وسائل إعلام)، وتحليل هذه المعلومات لتحديد طبيعة الأزمة وحجمها وتطورها المحتمل، وتحديد خيارات الاستجابة المتاحة وتقييم كل خيار من حيث الفعالية والتكلفة والآثار الجانبية، واتخاذ القرارات وتوجيه الفرق الميدانية لتنفيذها، ومتابعة تنفيذ القرارات وتعديلها حسب تطور الأحداث، والتواصل المستمر مع الإدارة العليا والجهات الخارجية والجمهور، وتوثيق كل خطوة وقرار. وتُعد جودة المعلومات وسرعة تدفقها من العوامل الحاسمة في نجاح العمليات، حيث أن القرار في غرفة العمليات لا يكون أفضل من المعلومات التي يُبنى عليها .

خامساً: التكامل مع غرف التحكم والعمليات الأخرى

لا تعمل غرفة عمليات إدارة الأزمات في عزلة، بل تتكامل وتتعاون مع غرف تحكم وعمليات أخرى داخل المنشأة وخارجها، لتشكل منظومة متكاملة لإدارة الطوارئ. ففي داخل المنشأة، تتكامل مع غرفة التحكم الأمنية التي تراقب أنظمة الأمن المادية والإلكترونية لحظياً، وغرفة التحكم التشغيلية التي تراقب العمليات الإنتاجية وتشغيل الأنظمة الحيوية، وغرفة التحكم التقنية) كغرفة تحكم الشبكات أو أنظمة SCADA). وتتشارك هذه الغرف المعلومات وتُنسق الاستجابة مع غرفة إدارة الأزمات، لتوفير صورة شاملة للموقف. وخارج المنشأة، تتكامل غرفة العمليات مع غرف عمليات الجهات الحكومية كالشرطة والدفاع المدني والإسعاف، وغرف

عمليات القطاعات الأخرى المرتبطة بالبنية التحتية، وغرف العمليات المركزية الوطنية في حالات الأزمات الكبرى. وقد أظهرت التجارب العملية، كالتمارين التي تجريها وزارة الدفاع الأمريكية على منشآتها، أن نجاح الاستجابة للأزمات يعتمد بشكل كبير على مدى التكامل والتنسيق بين غرفة العمليات والجهات المختلفة، وأن التمارين المشتركة التي تختبر هذا التكامل تُعد من أهم أدوات التحسين المستمر .

سادساً: التدريب والتمارين على عمليات غرفة العمليات

تظل غرفة العمليات مجرد مبنى وتجهيزات ما لم تُخضع كوادرها وأنظمتها لتدريبات وتمارين منتظمة تبني قدراتها وتكشف ثغراتها. وتشمل برامج التدريب تدريباً فردياً مستمراً لكل كادر على أدوات ومهام وظيفته، وتدريباً جماعياً على عمليات الفريق داخل الغرفة، وتدريبات على أجهزة المحاكاة التي تحاكي أزمات افتراضية معقدة، وتمارين طاولة (Tabletop) التي تناقش سيناريوهات وتختبر فهم الإجراءات والأدوار، وتمارين عملية محدودة تختبر عناصر معينة من عمليات الغرفة، وتمارين شاملة واسعة تشمل جميع عناصر المنشأة وتشارك فيها جهات خارجية. وتُستخدم هذه التمارين لتقييم كفاءة الكوادر، وفعالية الإجراءات، وسلامة أنظمة الاتصالات والمعلومات، وجاهزية التجهيزات التقنية، وقدرة الغرفة على التكيف مع سيناريوهات غير متوقعة. وتُجرى تمارين غرفة العمليات بشكل دوري ومنتظم (كتمارين شهرية أو ربع سنوية)، مع تمارين كبرى سنوية تشمل جميع الجهات، لضمان بقاء الجاهزية في أعلى مستوياتها. وقد أظهرت التجارب أن الفرق التي تُدرب بانتظام تستجيب بشكل أسرع وأكثر فعالية في الأزمات الحقيقية .

سابعاً: التحديات في إدارة غرفة العمليات

تواجه إدارة غرفة العمليات خلال الأزمات مجموعة من التحديات التي قد تعيق فعاليتها، وتستوجب الاستعداد المسبق للتعامل معها. ومن أبرز هذه التحديات ضغط المعلومات الهائل الذي يُمكن أن يؤدي إلى "شلل التحليل" وعدم القدرة على التمييز بين المهم وغير المهم، وفشل أو تعطل الأنظمة التقنية في أسوأ الأوقات (مما يُبرز أهمية التكرارية والتعددية في الأنظمة الحيوية)، وصعوبة اتخاذ القرارات في ظل

عدم اليقين ونقص المعلومات الكاملة، والصـــراعات التنظيمية بين الجهات المختلفة حول الصـلاحيات والمسـؤوليات، وصـعوبة التواصـل الفعال مع الجمهور ووسـائل الإعلام في خضـم الأزمة، والإرهاق النفسـي والجسـدي للكوادر التي تعمل لسـاعات طويلة تحت ضـــغط هائل. وللتغلب على هذه التحديات، تُســـتخدم أدوات وتقنيات متخصـصـــة كأنظمة دعم القرار، وأنظمة إدارة المعلومات التي تُصـنف الأولويات، وتُوضـع خطط لتناوب الفرق ومنع الإرهاق، وتُصـمم الإجراءات لتكون مرنة وقابلة للتكيف، وتُسـتفاد من الدروس المسـتفادة من الأزمات السـابقة لتحسـين الاسـتجابة للمستقبل .

ثامناً: التطورات المستقبلية في غرف عمليات إدارة الأزمات

تشـهد غرف عمليات إدارة الأزمات تطوراً متسـارعاً بفعل التقدم التكنولوجي، ومن المتوقع أن تشـــهد تحولات نوعية في الســـنوات القادمة. وتشـــمل هذه التطورات اسـتخدام الذكاء الاصـطناعي في تحليل كميات هائلة من البيانات في الوقت الفعلي، وتقديم توصيات لقادة الأزمات، والتنبؤ بتطور السيناريوهات، مما يُعزز قدرة صناع القرار على التصـرف بسـرعة ودقة أكبر .كما سـيؤدي دمج تقنيات التوأم الرقمي (Digital Twin)إلى خلق نسـخ افتراضـية للمنشـأة والأنظمة تسـمح بمحاكاة تأثير القرارات قبل تنفيذها في الواقع، وتُســتخدم الواقع المعزز والافتراضـــي في تدريب الكوادر وفي توجيه الفرق الميدانية أثناء الأزمات، كما سـتُصـبح أنظمة الاتصـالات الفضـــائية وتقنيات الجيل الخامس والســـادس أكثر انتشـــاراً لتوفير اتصـــالات فائقة السرعة والموثوقية، وستزدهر المنصـات السحابية لتوفير الوصـول إلى أنظمة غرفة العمليات من أي مكان، مما يُسهل العمل عن بُعد واستمرارية العمليات. وستُسهم هذه التطورات في جعل غرف العمليـات أكثر قدرة على التكيف والاســـتجابـة، وأكثر فعالية في حماية المنشآت الحيوية وضمان استمرارية الخدمات الحيوية للمجتمع .

وتُعد غرفة عمليات إدارة الأزمات بحق حجر الزاوية في منظومة إدارة المخاطر الأمنية، فهي المكان الذي تلتقي فيه الاســـتعدادات النظرية بالقدرات العملية، وتُتخذ فيه القرارات المصـيرية، وتُحول فيه الأزمات من تهديدات مدمرة إلى تحديات يمكن

احتواؤها وتجاوزها. وتتطلب فعالية هذه الغرفة اســتثماراً مســتمراً في التجهيزات والكوادر والتدريب، وإرادة قيادية تدعم ثقافة الاستعداد والتخطيط، وتكاملاً وثيقاً مع جميع الجهات المعنية داخل المنشــأة وخارجها، لضــمان أن تكون المنشــأة مســتعدة لمواجهة أي أزمة، مهما كان حجمها أو تعقيدها .

خطوات التعامل مع حالات الطوارئ

يُعد التعامل مع حالات الطوارئ التطبيق العملي الأكثر حسماً لمنظومة إدارة المخاطر الأمنية، فهو اللحظة التي تُختبر فيها جميع الخطط والإجراءات والتدريبات في مواجهة واقعية لا تقبل التأجيل أو التردد. وتتطلب حالات الطوارئ في المنشآت الحيوية استجابة سريعة ومنظمة، تجمع بين الحسم في اتخاذ القرارات، والمرونة في التكيف مع المتغيرات، والتنسيق المحكم بين جميع الأطراف المعنية. وتقوم خطوات التعامل مع حالات الطوارئ على منهجية واضحة ومتسلسلة، تبدأ باكتشاف الحالة والتبليغ عنها، وتمر بتقييم الموقف واتخاذ القرارات، وتنفيذ إجراءات الاستجابة، وانتهاء بمرحلة التعافي وتقييم الأداء، مع استمرارية عمليات الاتصال والتوثيق طوال مراحل الأزمة. وقد أثبتت التجارب العملية أن نجاح التعامل مع الطوارئ يعتمد بشكل كبير على مدى الاستعداد المسبق، وجودة التخطيط، وكفاءة التدريب، وسرعة اتخاذ القرارات في اللحظات الحرجة."1"

أولاً: الاكتشاف والتبليغ المبكر

تبدأ عملية التعامل مع حالات الطوارئ باكتشاف الحالة والتبليغ عنها بأسرع وقت ممكن، حيث أن سرعة الاكتشاف والتبليغ ترتبط ارتباطاً مباشراً بحجم الأضرار وفرص السيطرة على الموقف. وتشمل مصادر الاكتشاف أنظمة الكشف الآلية كأجهزة إنذار الحريق، وأجهزة كشف الغازات والتسربات، وأنظمة كشف التسلل والاختراق، وكاميرات المراقبة التي ترصد الأحداث غير العادية، بالإضافة إلى التبليغ البشري من قبل العاملين أو الزوار أو المارة الذين يلاحظون أي طارئ. وتُصمم أنظمة التبليغ لتكون سريعة وبسيطة، وتشمل أزرار الإنذار اليدوية المنتشرة في جميع أنحاء المنشأة، وخطوط الاتصال المباشرة بغرفة العمليات، وتطبيقات الهواتف الذكية المخصصة للتبليغ عن الطوارئ. ويُعد التبليغ الفعال نقطة البداية الحاسمة في سلسلة الاستجابة، إذ يجب أن يصل البلاغ إلى غرفة العمليات خلال ثوانٍ من اكتشاف الحالة، وأن يتضمن معلومات أولية عن طبيعة الطارئ، وموقعه، وحجمه التقريبي، وأي إصابات أولية، ليتمكن فريق الاستجابة من التحرك الفوري

وتوجيه الموارد المناسبة. ويُوصى بتدريب جميع العاملين على كيفية التبليغ عن الطوارئ، وإجراء اختبارات دورية لأنظمة التبليغ للتأكد من جاهزيتها وفعاليتها "2".

ثانياً: تقييم الموقف وتحديد مستوى الاستجابة

عند وصول البلاغ إلى غرفة العمليات، تبدأ مرحلة تقييم الموقف التي تُعد من أهم الخطوات في التعامل مع الطوارئ، إذ يُحدد على أساسها مستوى الاستجابة المطلوب ونوع الموارد التي سيتم تعبئتها. ويشمل التقييم جمع المعلومات من مصادر متعددة، كالتقارير الميدانية من الفرق الأولى التي تُرسل إلى الموقع، ومشاهدة كاميرات المراقبة، وقراءة بيانات أجهزة الاستشعار، والتواصل مع المبلغين للحصول على تفاصيل إضافية. ويُصنف الطارئ خلال هذه المرحلة وفق عدة معايير، كحجم الطارئ (بسيط، متوسط، كبير، كارثي)، ونوعه (حرائق، تسربات كيميائية، هجمات أمنية، كوارث طبيعية، وغيرها)، وسرعة تفاقمه، وتأثيره المحتمل على الأرواح والممتلكات والعمليات، والموارد المتاحة للتعامل معه. ويُستخدم نظام التصنيف لتحديد مستوى الاستجابة، فالمستوى الأول للطوارئ البسيطة التي يمكن التعامل معها بموارد المنشأة الذاتية، والمستوى الثاني للطوارئ المتوسطة التي تتطلب تعبئة موارد إضافية من المنشأة، والمستوى الثالث للطوارئ الكبرى التي تتطلب استدعاء جهات خارجية، والمستوى الرابع للكوارث التي تستدعي الاستجابة الوطنية الشاملة. ويُعد تحديد المستوى الصحيح بسرعة أمراً بالغ الأهمية، فالتقليل من شأن الطارئ قد يؤدي إلى نقص في الاستجابة، والمبالغة فيه قد تؤدي إلى استنزاف الموارد وإثارة الذعر غير المبرر."3"

ثالثاً: تنشيط غرفة العمليات وتشكيل فريق إدارة الأزمة

عند تحديد مستوى الاستجابة، تُنشط غرفة عمليات إدارة الأزمات وفق المستوى المطلوب، ويُشكل فريق إدارة الأزمة الذي يضم المختصين اللازمين للتعامل مع الطارئ. وتشمل عملية التنشيط استدعاء الأعضاء الأساسيين لفريق الأزمة (كقائد الأزمة، ومدير العمليات، وخبراء المجالات المعنية)، وتجهيز أنظمة الاتصالات

والمعلومات، وتفعيل لوحات العرض والشـــاشـــات، وتوزيع الأدوار والمهام على أعضـاء الفريق وفق خطط الطوارئ المعتمدة. ويُعد التشكيل السريع للفريق وتوزيع الأدوار بشــكل واضــح من عوامل النجاح الحاســمة، إذ يمنع الفوضـــى والارتباك ويضـــمن أن كل مســؤول يعرف بالضـــبط ما هو مطلوب منه. وتُســتخدم في هذه المرحلة قوائم تدقيق (Checklists) معدة مســـبقاً لكل نوع من أنواع الطوارئ، لتوجيه الفريق والتأكد من عدم إغفال أي خطوة أساسية. ويُوصـى بأن تكون غرفة العمليات في حالة تأهب دائم، وأن تُجرى تدريبات دورية على تنشـــيطها وتشـــكيل فرق الأزمة، لتقليل زمن الاستجابة في الحالات الحقيقية إلى أدنى حد ممكن."4"

رابعاً: تنفيذ إجراءات الاستجابة الفورية

بعد تنشـــيط غرفة العمليات وتشـــكيل فريق الأزمة، تبدأ مرحلة تنفيذ إجراءات الاســـتجابة الفورية التي تهدف إلى احتواء الطارئ ومنع تفاقمه، وحماية الأرواح والممتلكات. وتختلف هذه الإجراءات باختلاف نوع الطارئ، ولكنها تشـــمل عادةً إجراءات عامة كإخلاء المناطق المتضـــررة ونقل الأفراد إلى مواقع آمنة، وتفعيل أنظمة الإطفاء والاحتواء (كرشاشات الحريق، وصمامات العزل، وأنظمة التبريد)، وإغلاق أو عزل الأنظمة المتضـررة لمنع انتشـار الضـرر، وتوجيه الفرق الميدانية إلى مواقع محددة للتدخل، وتوفير الإسعافات الأولية للمصـابين واستدعاء الإسعاف للحالات الخطيرة، والتواصـــل مع الجهات الخارجية كالدفاع المدني والشـــرطة والإســـعاف لطلب الدعم عند الحاجة. وتُنفذ هذه الإجراءات وفق خطط وإجراءات تشغيلية موحدة (SOPs) مُعدة مسبقاً لكل نوع من الطوارئ، ويُشرف على تنفيذها مدير العمليات في غرفة العمليات، مع متابعة مســـتمرة لتطور الموقف وتعديل الإجراءات حســب الحاجة. ويُعد التنســيق بين الفرق الميدانية وغرفة العمليات أمراً حيوياً في هذه المرحلة، لضـــمان أن الجهود تبذل في الاتجاه الصـــحيح وأن الموارد تُستخدم بكفاءة."5"

خامساً: التنسيق مع الجهات الخارجية

تتطلب العديد من حالات الطوارئ في المنشـــآت الحيوية تنســـيقاً وثيقاً مع جهات خارجية، ســـواء لتوفير دعم إضـــافي أو لتنســـيق الجهود المشـــتركة أو للامتثال للمتطلبات القانونية والتنظيمية. وتشـــمل هذه الجهات الدفاع المدني والإســـعاف والشـرطة، والجهات التنظيمية الحكومية كوزارة الصـحة أو هيئة الطاقة، والجهات الأمنية والاسـتخبارية، والسـلطات المحلية، والمنشـآت المجاورة المتأثرة، ووسـائل الإعلام عند الحاجة. وتُستخدم في عملية التنسيق قنوات اتصـال محددة ومتفق عليها مســـبقاً، وبروتوكولات موحدة للتعامل مع كل جهة، وغالباً ما تُنشـــأ مراكز قيادة مشتركة في الأزمات الكبرى تجمع ممثلين عن جميع الأطراف. ويُعد التنسيق الفعال مع الجهـات الخـارجيـة أحـد أهم عوامـل نجـاح الاســـتجـابـة للطوارئ، فهو يمنع الازدواجية ويضـــمن توزيع الموارد بكفاءة، ويوفر للجهات الخارجية الصـــورة الصـــحيحة عن الموقف لتتمكن من تقديم الدعم المناســـب. وقد أظهرت تجارب المنشـآت التي تعرضـت لأزمات كبرى أن التنسـيق المسـبق والعلاقات الجيدة مع الجهات الخارجية كان من أهم عوامل تجاوز الأزمة بأقل الخســائر، وأن غياب هذا التنسيق يُعد من أخطر نقاط الضعف في أي منظومة لإدارة الطوارئ."6"

سادساً: التواصل الداخلي والخارجي وإدارة الإعلام

يُعد التواصل أثناء الطوارئ من أكثر العمليات حساسية وتأثيراً في مسار الأزمة، إذ أن التواصـل الجيد يبني الثقة ويقلل الذعر ويُسـهل عمليات الاسـتجابة، في حين أن التواصـل السـيء قد يُضـاعف الأزمة ويُحدث فوضـى إضـافية. ويشـمل التواصـل الـداخلي إبقـاء جميع العـاملين على علم بتطورات الموقف، وتوجيههم بـإجراءات السـلامة المطلوبة، والإجابة على اسـتفسـاراتهم، وتقديم الدعم النفسـي عند الحاجة. ويشمل التواصل الخارجي إعلام أسر العاملين، والتواصل مع وسائل الإعلام لتقديم معلومات دقيقة وموثوقة، والتعامل مع اســـتفســـارات الجمهور والجهات المعنية، وتصـحيح أي معلومات مغلوطة أو شـائعات قد تنتشـر. وتُدار عمليات التواصـل عادةً من قبل فريق متخصص في غرفة العمليات، يعمل وفق خطة اتصـالات مُعدة مسبقاً،

ويُراعي في تعاملاته مبادئ الشفافية والصدق والسرعة، مع الحفاظ على المعلومات الحساسة التي قد تضر بالأمن أو التحقيقات. ويُوصى بتدريب المتحدثين الرسميين على التعامل مع وسائل الإعلام في أوقات الأزمات، وإجراء تمارين محاكاة للإعلام كجزء من التمارين الأمنية الشاملة."7"

سابعاً: إدارة الموارد واللوجستيات خلال الطوارئ

تعتمد فعالية الاستجابة للطوارئ بشكل كبير على توفر الموارد المناسبة في الوقت والمكان المناسبين، مما يجعل إدارة الموارد واللوجستيات أحد الأعمدة الأساسية في التعامل مع حالات الطوارئ. وتشمل الموارد المطلوبة خلال الطوارئ الموارد البشرية كفرق الاستجابة المتخصصة والإسعافية والدعم، والمعدات كسيارات الإطفاء والإسعاف ومعدات الإنقاذ وأجهزة الكشف، والمواد الاستهلاكية كمواد الإطفاء والمطهرات والمستلزمات الطبية، والمرافق كغرف العمليات ومراكز الإيواء الطارئ ومخازن الطوارئ. وتُدار هذه الموارد من خلال نظام لوجستي متكامل يبدأ بتقييم الاحتياجات، ثم تحديد المصادر المتاحة داخلياً والمطلوب استجلابها خارجياً، ثم توجيه الموارد إلى حيث تحتاج، ومتابعة استخدامها وتجديدها عند الحاجة. وتُستخدم في هذه العملية أنظمة تتبع الموارد، وقوائم جرد محدثة، وعقود مسبقة مع موردين للطوارئ، واتفاقيات دعم متبادل مع منشآت مجاورة. وقد أثبتت التجارب أن نقص الموارد أو سوء توزيعها يُعد من أكثر أسباب فشل الاستجابة للطوارئ شيوعاً، مما يستوجب استثماراً كافياً في التجهيز للطوارئ وتدريب الفرق اللوجستية على إدارة الموارد في ظل الضغط والارتباك."8"

ثامناً: التعافي والعودة إلى العمليات الطبيعية

بعد السيطرة على الطارئ واحتوائه، تبدأ مرحلة التعافي التي تهدف إلى إعادة المنشأة إلى حالتها الطبيعية بأسرع وقت ممكن، مع ضمان استمرارية العمليات الحيوية خلال فترة التعافي. وتشمل هذه المرحلة عدة عمليات متداخلة، كتقييم الأضرار وتحديد أولويات الإصلاح، وإعادة تشغيل الأنظمة المتوقفة تدريجياً، وإصلاح وتأهيل البنية التحتية المتضررة، وتعويض المتضررين ودعم الفرق

المتعبة، وتحليل الحادث واســـتخلاص الدروس، وتحديث الخطط والإجراءات بناءً على الدروس المســتفادة. وتُعد خطة اســتمرارية العمل (BCP) وخطة التعافي من الكوارث (DRP) الأدوات الأســاســية في هذه المرحلة، إذ تُحدد كيفية اســتمرار الوظائف الحيوية خلال فترة التعافي وكيفية العودة التدريجية إلى الحالة الطبيعية. ويُوصـــى بأن تكون مرحلة التعافي جزءاً مدمجاً من خطط الطوارئ، وأن تُختبر وتُمارس بشكل دوري كباقي مراحل الاستجابة، لضمان عدم إغفال تحديات التعافي التي قد تكون مختلفة عن تحديات الاستجابة الفورية وتتطلب موارد وخططاً خاصة "9".

تاسعاً: تقييم الأداء واستخلاص الدروس

تُعد مرحلة تقييم الأداء واســـتخلاص الدروس من أهم مراحل التعامل مع حالات الطوارئ، رغم أنها غالباً ما تُهمل تحت ضـغط العودة إلى العمل الروتيني. وتشـمل هذه المرحلة إجراء مراجعة شاملة للاستجابة بعد انتهاء الأزمة (Post-Incident Review)، يتم خلالها تحليل ما حدث وما كان يجب أن يحدث، وتحديد نقاط القوة التي ينبغي تعزيزها، ونقاط الضـــعف التي تســـتوجب المعالجة، وتقييم أداء جميع الأطراف المشـــاركة (الداخلية والخارجية)، وتقييم فعالية الخطط والإجراءات والأنظمة والتجهيزات، وتقييم جودة اتخاذ القرارات والتواصـــل، وتحديد الدروس المستفادة وتوصيات التحسين. وتُستخدم في هذه العملية أدوات متعددة كالمقابلات مع المشاركين، وتحليل السجلات والتسجيلات، والاستبيانات، وورش العمل المشتركة. وتُنتج عن هذه المراجعة تقرير تقييم شـــامل يحتوي على توصـــيات محددة وقابلة للتنفيذ، وتُتابع عملية تنفيذ هذه التوصيات من خلال خطة تحسين واضحة. وقد أثبتت الدراسات أن المنشآت التي تُجري مراجعات ما بعد الأزمات بجدية وتنفذ توصياتها تتحســن اســتجابتها للطوارئ بشــكل مطرد مع كل أزمة، بينما تلك التي تهمل هذه المرحلة تكرر أخطاءها مراراً وتظل عرضة لنفس المخاطر."10"

عاشراً: التحسين المستمر لخطط وإجراءات الطوارئ

تتسم بيئة المخاطر التي تواجه المنشآت الحيوية بالتغير المستمر، مما يستوجب تحديثاً مستمراً لخطط وإجراءات الطوارئ لمواكبة هذه التغيرات. ويعتمد التحسين المستمر على عدة مصادر رئيسية، كالدروس المستفادة من الحوادث السابقة في المنشأة نفسها، والدروس المستفادة من حوادث منشآت مماثلة، والتغيرات في بيئة التهديدات كظهور تهديدات جديدة أو تطور تهديدات قائمة، والتغيرات في المنشأة نفسها كتوسع العمليات أو إدخال تقنيات جديدة أو تغير الهيكل التنظيمي، والتطورات التكنولوجية في أنظمة الكشف والاستجابة، والممارسات الفضلى الجديدة في مجال إدارة الطوارئ، وتوصيات الجهات التنظيمية والخبراء. ويُوصى بإنشاء آلية منهجية لمراجعة وتحديث خطط الطوارئ بشكل دوري (كمراجعة سنوية على الأقل)، مع تحديثات عند الحاجة كلما طرأت تغيرات كبيرة. وتُستخدم في هذه العملية أدوات كقوائم المراجعة وتقييم المخاطر المحدثة وتحليل الفجوات، ويُشارك فيها جميع الأطراف المعنية لضمان شمولية التحديث وملاءمته للواقع العملي. ويُعد التحسين المستمر لخطط وإجراءات الطوارئ استثماراً في المستقبل، إذ يضمن أن تظل المنشأة مستعدة لمواجهة التحديات الجديدة والمتطورة، ولا تعتمد على خطط قد تكون تجاوزها الزمن أو لم تعد متناسبة مع واقع التهديدات الحالي."11"

وتُشكل خطوات التعامل مع حالات الطوارئ العنصر الأكثر ديناميكية وحساسية في منظومة إدارة المخاطر الأمنية، إذ تمثل اللحظة التي يُختبر فيها كل ما تم التخطيط له وتدريبه. وتتطلب هذه الخطوات توازناً دقيقاً بين الالتزام بالخطط المعدة مسبقاً والمرونة في التكيف مع تطورات الموقف، بين السرعة في اتخاذ القرارات والدقة في تنفيذها، بين المركزية في القيادة واللامركزية في التنفيذ. وعندما تُدار هذه الخطوات بكفاءة، فإنها تحول الأزمة إلى تحدٍ يمكن تجاوزه، وتحافظ على سلامة الأفراد واستمرارية العمليات الحيوية، وتعزز ثقة الجميع في قدرة المنشأة على الصمود في وجه المخاطر. وتظل هذه القدرة رهناً بالاستثمار المستمر في التخطيط والتدريب والتجهيز، وبالثقافة الأمنية التي تجعل الاستعداد للطوارئ جزءاً من الحمض النووي للمنشأة وليس مجرد إجراءات شكلية تُتبع عند الضرورة."12"

إجراءات الإخلاء في الحالات الطارئة

يُعد الإخلاء في الحالات الطارئة أحد أهم إجراءات حماية الأرواح في المنشـــآت الحيوية، فهو التدبير الذي يُتخذ لنقل الأفراد من مناطق الخطر إلى مناطق آمنة عند وقوع أي طارئ يهدد ســـلامتهم. وتكتســـب إجراءات الإخلاء أهمية خاصـــة في المنشـــآت الحيوية نظراً لكثافة العاملين فيها، وتعقيد تصـــميماتها المعمارية، ووجود مواد خطرة قد تزيد من خطورة البقاء في الموقع، وصـــعوبة الوصـــول إلى بعض مرافقها في أوقات الطوارئ. وتقوم إجراءات الإخلاء الفعالة على التخطيط المسبق، والتدريب المنتظم، والتواصل الواضح، والقيادة الحازمة، والتقييم المستمر، لضمان أن يتم الإخلاء بأسـرع وقت ممكن وبأقل قدر من الفوضـى والإصـابات. وقد أثبتت التجارب العملية أن الإخلاء المنظم والمدرب عليه يمكن أن يقلل زمن الإخلاء بنسبة تصـــل إلى ٥٠٪ مقارنة بالإخلاء العشـــوائي، مما يُحدث فرقاً حاســـماً بين النجاة والمأساة في الحالات الطارئة."1"

أولاً: أنواع الإخلاء ومستوياته

تتنوع إجراءات الإخلاء في المنشـــآت الحيوية لتتناســـب مع طبيعة الطارئ وحجمه وموقعه، وتُصـنف عادةً إلى ثلاثة أنواع رئيسـية: الإخلاء الكلي، والإخلاء الجزئي، والإخلاء الأفقي. فالإخلاء الكلي يُســـتخدم في حالات الطوارئ الكبرى التي تهدد المنشـأة بأكملها، كالحرائق الواسـعة، أو الانفجارات الكبيرة، أو التسـربات الكيميائية الشـــديدة، أو الكوارث الطبيعية التي تؤثر على كامل المبنى، ويتطلب إخلاء جميع الأفراد إلى نقاط التجمع الخارجية البعيدة عن المنشـأة. أما الإخلاء الجزئي فيُسـتخدم في الحالات التي تقتصـر فيها خطورة الطارئ على جزء معين من المنشـأة، كحريق في طابق معين، أو تســـرب في مبنى محدد، أو تهديد في منطقة محددة، ويقتصـــر على إخلاء الأفراد من المنطقة المتضـــررة والمناطق المجاورة لها مع إبقاء بقية المنشـــأة في حالة تشـــغيل طبيعي أو تأهب. ويُعد الإخلاء الأفقي من أكثر أنواع الإخلاء شـيوعاً في المباني متعددة الطوابق، حيث يُنقل الأفراد من الطابق المتضـرر إلى طـابق آخر أكثر أمـانـاً في نفس المبنى، عبر ممرات آمنـة، دون الحـاجـة إلى

الخروج من المبنى بالكامل، ويُستخدم غالباً في حالات الحرائق المحدودة أو التسريبات الموضعية. ويُحدد نوع الإخلاء المناسب بناءً على تقييم سريع للموقف من قبل فريق إدارة الأزمة، مع مراعاة أن القرار يجب أن يُتخذ بسرعة وحسم، وأن يُبلغ لجميع المعنيين بشكل واضح وغير قابل للبس."2"

ثانياً: تخطيط مسارات الإخلاء ومخارجه

يُعد تخطيط مسارات الإخلاء ومخارجه من العناصر الأساسية لنجاح أي عملية إخلاء، إذ يجب أن تكون هذه المسارات آمنة وسهلة الوصول ومناسبة لجميع فئات الأفراد، بما في ذلك ذوي الاحتياجات الخاصة. وتشمل متطلبات تخطيط المسارات توفير مخارج طوارئ كافية وموزعة بشكل يضمن وصول جميع الأفراد إلى مخرج خلال مسافة آمنة (كحد أقصى ٣٠-٤٥ متراً في المباني التجارية والصناعية)، وتصميم المسارات لتكون واضحة ومباشرة وخالية من العوائق، مع ممرات ذات عرض كافٍ لاستيعاب كثافة الأفراد المتوقعة (عادةً ١,٢ متر على الأقل للممرات الرئيسية)، وإضاءة طوارئ مستقلة تضيء المسارات في حال انقطاع التيار الكهربائي، وعلامات إرشادية مضيئة وموجّهة نحو المخارج، وأبواب طوارئ تفتح باتجاه الخارج بسهولة (بدون مفتاح) وتكون مزودة بقضبان دفع (Panic Bars) تسمح بفتحها بالضغط من الداخل. وتُستخدم مواد مقاومة للحريق في إنشاء ممرات الإخلاء (كالأبواب المقاومة للحريق لمدة ٦٠-٩٠ دقيقة على الأقل)، وتُصمم المسارات لتكون محمية من الدخان والحرارة والمواد الخطرة، وتُفصل مسارات الإخلاء عن المناطق التي قد تحتوي على مواد خطرة أو معدات ثقيلة قد تسقط أثناء الطارئ. ويُوصى بإجراء مراجعات دورية لمسارات الإخلاء للتأكد من بقائها خالية من العوائق، وأن الأبواب تعمل بشكل سليم، وأن الإضاءة والعلامات في حالة جيدة "3".

ثالثاً: خطة الإخلاء وإجراءاتها التشغيلية

تُعد خطة الإخلاء وثيقة شاملة تُحدد كافة الإجراءات الواجب اتباعها عند تنفيذ عملية الإخلاء، وتُوزع على جميع الإدارات والأقسام، وتُدرَّب عليها الفرق بشكل دوري.

وتتضـمن الخطة عادةً فريق إدارة الإخلاء الذي يضـم قائد الإخلاء (المسـؤول عن القيادة العامة واتخاذ القرارات)، ومنسـقي الطوابق أو المناطق (المسـؤولون عن توجيه الإخلاء في مناطقهم)، وفرق المسـاعدة (المسـؤولون عن مسـاعدة ذوي الاحتياجات الخاصـة)، وفرق التفتيش (المسـؤولون عن التأكد من إخلاء جميع المناطق)، وفرق الاتصـال (المسـؤولون عن التواصـل مع غرفة العمليات والجهات الخارجية). وتشـمل الخطة أيضـاً آليات الإنذار والتوجيه، كأنظمة الإنذار الصـوتية والمرئية التي تُطلق إشـارات محددة للإخلاء، وأنظمة الاتصـال الجماعي للطوارئ (كتطبيقات الهواتف أو الرسـائل النصـية أو أجهزة اللاسـلكي)، وتعليمات واضـحة ومبسـطة للموظفين حول ما يجب فعله عند سـماع إنذار الإخلاء. وتُحدد الخطة نقاط التجمع الآمنة خارج المبنى، بعيدة عن مناطق الخطر (على بعد ٥٠ متراً على الأقل في المباني العادية، وأكثر في المنشـآت التي تتعامل مع مواد خطرة)، وتُجهز هذه النقاط بوسائل إسعاف أولي واتصـال، وتُخصـص مسؤولاً للتأكد من وصـول الجميع إلى نقاط التجمع وإجراء إحصـاء دقيق للأفراد. كما تشـمل الخطة إجراءات التعامل مع الحالات الخاصـة كالأفراد ذوي الإعاقة أو المصـابين، والزوار غير الملمين بتصـميم المنشـأة، والعاملين في المناطق المعزولة أو تحت الأرض، والمواد الخطرة التي قد تتطلب إجراءات إخلاء خاصة."4"

رابعاً: آلية الإنذار والتوجيه أثناء الإخلاء

يُعد الإنذار الواضـح والفعال شـرطاً أسـاسـياً لنجاح عملية الإخلاء، إذ يجب أن يُعلم جميع الأفراد بـالحـالـة الطـارئـة وبنوع الإخلاء المطلوب في أسـرع وقت ممكن. وتشـمل آليات الإنذار أنظمة الإنذار الصـوتية (كصـفارات الإنذار والجرس وأجهزة البث الصـوتي) التي تُطلق نغمات أو رسـائل مسـجلة أو حية تُحدد نوع الطارئ والإجراء المطلوب، وأنظمـة الإنـذار المرئيـة (كـالأضـواء الوامضـة واللافتـات الإلكترونية وشاشات العرض) التي تُكمل الإنذار الصوتي، خاصة في الأماكن عالية الضوضاء أو للأفراد ذوي الإعاقات السمعية، وأنظمة الاتصال الجماعي (كتطبيقات الهواتف الذكية والرسـائل النصـية والبريد الإلكتروني) التي تُوفر تعليمات مفصـلة

للأفراد أثناء الإخلاء، مع مراعاة أن تكون هذه الأنظمة مزودة بمصادر طاقة احتياطية لضمان عملها عند انقطاع التيار الكهربائي. ويُوصى باستخدام رسائل إنذار موحدة وواضحة، تتضمن نوع الطارئ، والإجراء المطلوب (إخلاء كلي، جزئي، أفقي)، ومسار الإخلاء الموصى به، ونقطة التجمع المحددة، وتعليمات إضافية كعدم استخدام المصاعد، وترك المتعلقات، ومساعدة الآخرين. وتُجرى اختبارات دورية لأنظمة الإنذار، وتُدرَّب الفرق على استخدامها، ويُطلب من العاملين التعرف على أصوات الإنذار المختلفة وتمييزها."5"

خامساً: تدريب العاملين على إجراءات الإخلاء

يُعد تدريب العاملين على إجراءات الإخلاء من أهم عوامل نجاح أي عملية إخلاء، إذ أن الأفراد المدربين يستجيبون بشكل أسرع وأكثر تنظيماً من غير المدربين، ويُقللون من احتمالية الذعر والفوضى. وتشمل برامج التدريب تعريف جميع العاملين بخطة الإخلاء ومساراتها ومخارجها ونقاط التجمع، وتدريبهم على التصرف الصحيح عند سماع إنذار الإخلاء (كالتوقف عن العمل فوراً، وإغلاق المعدات إن أمكن، والتوجه إلى أقرب مخرج آمن، وعدم استخدام المصاعد، ومساعدة الآخرين)، وتدريب فرق الإخلاء المتخصصة (كقادة الإخلاء ومنسقي الطوابق وفرق المساعدة) على أدوارهم ومسؤولياتهم، وإجراء تمارين إخلاء دورية (كتمارين ربع سنوية على الأقل) تشمل جميع العاملين، مع تنويع سيناريوهات التمارين لتشمل أوقاتاً مختلفة وظروفاً متنوعة (كليل، نهار، عطلات نهاية الأسبوع، في وجود زوار). ويُوصى بتسجيل ومتابعة أداء العاملين في تمارين الإخلاء، وتقييم وقت الإخلاء ومقارنته بالمعايير الموضوعة، وتحديد المناطق التي تتطلب تحسيناً، وتقديم تغذية راجعة للعاملين عن أدائهم، وتحديث خطة الإخلاء بناءً على الدروس المستفادة من التمارين. وقد أظهرت الدراسات أن المنشآت التي تُجري تمارين إخلاء منتظمة تحقق أوقات إخلاء أقصر بكثير من تلك التي لا تُجريها، وتكون أكثر قدرة على حماية أرواح العاملين في الحالات الطارئة الحقيقية."6"

سادساً: إدارة الحشود والتحكم في التدفق أثناء الإخلاء

تُعد إدارة الحشـــود والتحكم في تدفق الأفراد أثناء الإخلاء من التحديات الكبرى، خاصـة في المنشآت الكبيرة التي تضم أعداداً كبيرة من العاملين أو الزوار. وتشمل إجراءات إدارة الحشـود توجيه الأفراد عبر مسـارات محددة مسـبقاً لتجنب الازدحام عند المخـارج، واســـتخدام الحواجز المؤقتـة واللافتـات لتوجيـه الحركـة، وتوزيع المخارج بشكل يمنع تكدس جميع الأفراد على مخرج واحد، وتدريب منسقي الإخلاء على توجيه الحشـــود ومنع التدافع، واســـتخدام أنظمة العد الإلكتروني لتتبع أعداد المغادرين والتأكد من إخلاء الجميع، وتطبيق نظام الأولوية في الإخلاء بحيث تُعطى الأولوية للأفراد الأكثر عرضـــة للخطر (كالمصـــابين وذوي الاحتياجات الخاصـــة والعاملين في المناطق الأكثر خطورة). ويُوصـــى بتصـــميم المخارج والمســـارات لتكون قادرة على اسـتيعاب الكثافة المتوقعة (بمعدل ١,٠-٠,٥ متر مربع للشـخص الواحد في مناطق الانتظار)، واســـتخدام أنظمة المراقبة لتتبع حركة الأفراد وتحديد نقاط الازدحام، وإجراء تدريبات خاصـة لإدارة الحشـود للفرق المكلفة بهذه المهمة. وقد أظهرت تحليلات الحوادث أن سوء إدارة الحشود يُعد من أهم أسباب الإصابات والوفيات في عمليات الإخلاء، مما يؤكد أهمية الاســـتثمار في هذا الجانب من التخطيط والتدريب."7"

سابعاً: إجراءات الإخلاء الخاصة بالفئات ذات الاحتياجات الخاصة

تتطلب الفئات ذات الاحتياجات الخاصـــة (كذوي الإعاقات الجســـدية أو الحســـية أو العقلية، وكبار الســـن، والحوامل، والمصـــابين) إجراءات إخلاء خاصـــة تضـــمن ســـلامتهم وكرامتهم، ويجب أن تُدمج هذه الإجراءات في خطة الإخلاء الشـــاملة. وتشـــمل هذه الإجراءات تحديد أماكن تواجد هذه الفئات في المنشـــأة وتســـجيلهم في ســجلات خاصــة، وتوفير وســائل مســاعدة للإخلاء كالكراســي المتحركة الخاصــة للإخلاء، والمصـاعد المخصـصـة للطوارئ (في بعض التصـميمات الحديثة) والتي تُستخدم حصـراً لهذه الفئات تحت إشـراف مباشـر، ومناطق انتظار آمنة (Areas of Refuge) داخل المبنى يمكن لهذه الفئات الانتظار فيها لحين وصـــول فرق الإنقاذ، مع تزويد هذه المناطق بأنظمة اتصـال للتواصـل مع غرفة العمليات، وتعيين

مرافقين مدربين لمساعدة هذه الفئات أثناء الإخلاء، والتنسيق مع فرق الإسعاف والإنقاذ الخارجية لتوفير دعم إضافي. ويُوصى بإشراك ممثلين عن هذه الفئات في تخطيط وتقييم إجراءات الإخلاء، للتأكد من ملاءمتها وفعاليتها، وإجراء تدريبات خاصة تستهدف هذه الفئات ومرافقيها، وتقييم هذه الإجراءات بعد كل تمرين أو حادث فعلي للتأكد من أنها تلبي الاحتياجات الفعلية. وتُعد مسؤولية حماية الفئات الأكثر ضعفاً مؤشراً على نضج الثقافة الأمنية في المنشأة، وتستوجب عناية وتخطيطاً استثنائيين."8"

ثامناً: إجراءات ما بعد الإخلاء

لا تنتهي عملية الإخلاء بخروج آخر فرد من المبنى، بل تليها مرحلة ما بعد الإخلاء التي تشمل إجراءات حاسمة لضمان سلامة الجميع واستمرارية إدارة الأزمة. وتشمل هذه الإجراءات إجراء إحصاء دقيق للأفراد عند نقاط التجمع، للتأكد من خروج الجميع وتحديد أي مفقودين، وتقديم الإسعافات الأولية للمصابين واستدعاء الإسعاف للحالات الخطيرة، وتوفير الدعم النفسي للأفراد المصابين بالصدمة أو القلق، وتقييم فعالية عملية الإخلاء وجمع الملاحظات من المشاركين، والتنسيق مع الجهات الخارجية (كالإسعاف والدفاع المدني) لتقييم الموقف وتحديد الخطوات التالية، واتخاذ قرار بشأن متى يُسمح بالعودة إلى المبنى (بعد التأكد من زوال الخطر)، وتوثيق عملية الإخلاء بالكامل للاستفادة منها في التحسين المستقبلي. ويُعد الإحصاء الدقيق للأفراد من أكثر الإجراءات تحدياً في هذه المرحلة، خاصة في المنشآت الكبيرة التي تضم زواراً ومقاولين، ولذا يُوصى باستخدام أنظمة تسجيل الدخول والخروج الإلكترونية التي تُسهل تتبع الأفراد، وتدريب منسقي نقاط التجمع على إجراء الإحصاء بسرعة ودقة. وقد أظهرت التجارب أن ضعف إجراءات ما بعد الإخلاء، كعدم القدرة على إحصاء الأفراد بسرعة، قد يؤدي إلى استمرار حالة الذعر وإعاقة جهود الإنقاذ، مما يستوجب إيلاء هذه المرحلة الاهتمام نفسه الذي تولى للإخلاء نفسه."9"

تاسعاً: التحديات في تنفيذ إجراءات الإخلاء

تواجه المنشـــآت الحيوية مجموعة من التحديات في تنفيذ إجراءات الإخلاء، تتطلب وعياً مسبقاً وتخطيطاً لتجاوزها. ومن أبرز هذه التحديات حالة الذعر التي قد تصيب الأفراد، خاصـــة إذا لم يكونوا مدربين أو إذا فاجأهم الطارئ، حيث قد يؤدي الذعر إلى ســـلوكيات غير عقلانية كالتزاحم أو الركض في الاتجاه الخاطئ أو تجاهل التعليمات، مما يبطئ الإخلاء ويزيد الإصـــابات. ويُمثل ضـــعف الوعي بمســـارات الإخلاء تحدياً آخر، خاصـة في المنشـآت الكبيرة أو تلك التي تشـهد تغيرات متكررة في التوزيع المكاني، حيث قد لا يعرف العاملون الجدد أو الزوار أين توجد المخارج. كما قد تُعيق العوائق المادية (كالأثاث، الصـــناديق، المعدات) مســـارات الإخلاء، خاصـــة إذا لم تُراجع وتُزال بانتظام، أو قد تتعطل الأنظمة (كالإضـــاءة، الإنذار، الأبواب) في وقت الحاجة، مما يزيد من صـــعوبة الإخلاء. ويُشـــكل إخلاء ذوي الاحتياجات الخاصـة تحدياً إضـافياً، إذ تتطلب إجراءات خاصـة قد لا تكون متاحة أو مدربة بشكل كافٍ، وقد يكون تنسيق الإخلاء مع الجهات الخارجية (كالدفاع المدني) صـــعباً في اللحظات الحرجة، خاصـــة إذا كانت قنوات الاتصـــال غير واضـــحة أو مجربة مســـبقاً. وللتغلب على هذه التحديات، يُوصـــى بالتدريب المنتظم للجميع، والمراجعة الدورية لمســـارات الإخلاء، والصـــيانة المســـتمرة للأنظمة، والتخطيط الخاص للفئات الأكثر ضعفاً، وإجراء تمارين مشتركة مع الجهات الخارجية بانتظام "10".

عاشراً: التحسين المستمر لإجراءات الإخلاء

تُعد إجراءات الإخلاء نظاماً حياً يتطلب تحديثاً وتحسيناً مستمرين لمواكبة التغيرات في المنشأة وبيئة المخاطر. ويعتمد التحسين المستمر على مصادر متعددة، كالدروس المســـتفادة من تمارين الإخلاء الدورية، والدروس المســـتفادة من الحوادث الفعلية (سـواء في المنشـأة نفسـها أو في منشـآت مماثلة)، والتغيرات في تصـميم المنشـأة أو توزيع العـاملين، والتغيرات في طبيعـة المخـاطر المحتملـة، والتطورات في تقنيـات وأنظمـة الإنـذار والإخلاء، والتوصـــيات الجديدة من الجهـات التنظيميـة والمعـايير

الدولية، وآراء وملاحظات العاملين أنفســـهم الذين قد يكون لديهم اقتراحات عملية لتحسين الإجراءات. ويُوصـى بإنشـاء آلية منهجية لجمع وتحليل المعلومات المتعلقة بالإخلاء، وتحديث خطة الإخلاء والإجراءات المرتبطة بها بشكل دوري (كمراجعة ســـنوية على الأقل أو بعد كل حادث أو تمرين كبير)، وإجراء اختبارات دورية للمعدات والأنظمة المستخدمة في الإخلاء، وتدريب العاملين الجدد على الإجراءات المحدثة، وتقييم فعالية التحسينات التي تم تنفيذها في التمارين التالية. ويُعد التحسين المستمر لإجراءات الإخلاء التزاماً أخلاقياً وقانونياً تجاه سلامة الأفراد، واستثماراً في حماية أثمن ما تملكه المنشأة من أصول، وهو العنصر البشري."11"

وتُعد إجراءات الإخلاء في الحالات الطارئة من أهم مظاهر الجاهزية الأمنية في المنشآت الحيوية، فهي الإجراء الذي يُترجم فيه الالتزام بسلامة الأفراد إلى خطوات عملية ملموســـة. وتتطلب هذه الإجراءات توازناً بين التخطيط الهندســـي الدقيق، والتدريب البشري المستمر، والتواصل الفعال، والتقييم المنتظم، والتحسين المستمر. وعندما تُصمم وتُنفذ هذه الإجراءات بكفاءة، فإنها لا تحمي الأرواح فحسب، بل تبني الثقة بين العاملين، وتعزز ثقافة الســلامة الأمنية في المنشــأة، وتؤكد التزامها بأعلى معايير حماية الإنسان التي هي الغاية الأسمى لأي نظام أمني."12"

فرق الاستجابة السريعة

تمثل فرق الاستجابة السريعة التجسيد العملي لمبدأ الجاهزية في منظومة إدارة المخاطر الأمنية، فهي الوحدات المتخصصة المدربة والمجهزة للتحرك الفوري عند وقوع أي طارئ، بهدف احتواء الموقف، وتقليل الأضرار، واستعادة النظام في أقصر وقت ممكن. وتختلف فرق الاستجابة السريعة عن فرق الأمن الروتينية في كونها مُعدة خصيصاً للتعامل مع حالات الطوارئ غير المتوقعة، وتتمتع بقدرات خاصة تمكنها من التصرف تحت الضغط وفي ظروف استثنائية. وتتسم هذه الفرق بالمرونة، وسرعة رد الفعل، والتخصص الدقيق في مجالات محددة كالحرائق، أو التسربات الكيميائية، أو الهجمات السيبرانية، أو الاقتحامات الأمنية، أو الكوارث الطبيعية. ويُعد إنشاء وتدريب وتجهيز فرق الاستجابة السريعة استثماراً استراتيجياً يضمن للمنشأة القدرة على التعامل مع الأزمات بكفاءة واحترافية، ويُحدث الفارق الحاسم بين حادث يتم احتواؤه بسرعة وكارثة تتفاقم آثارها."1"

أولاً: مفهوم فرق الاستجابة السريعة وأنواعها

تُعرّف فرق الاستجابة السريعة في سياق أمن المنشآت الحيوية بأنها مجموعات بشرية مدربة ومنظمة ومجهزة، تعمل تحت قيادة موحدة، وتكون في حالة تأهب دائم للتحرك الفوري عند وقوع أي طارئ أمني أو تشغيلي يهدد سلامة الأفراد أو استمرارية العمليات. وتتنوع هذه الفرق بحسب طبيعة المخاطر التي صُممت لمواجهتها، وتشمل فرق الاستجابة للحرائق، المدربة على مكافحة الحرائق بأنواعها وإجراء عمليات الإخلاء والإطفاء، وفرق الاستجابة للتسريبات الكيميائية أو الإشعاعية، المتخصصة في التعامل مع المواد الخطرة واحتوائها ومنع انتشارها، وفرق الاستجابة الأمنية، المدربة على التعامل مع الاقتحامات والهجمات المسلحة والتهديدات الإرهابية، وفرق الاستجابة السيبرانية، المتخصصة في التعامل مع الاختراقات الإلكترونية وهجمات القرصنة واستعادة الأنظمة، وفرق الاستجابة الطبية، المدربة على تقديم الإسعافات الأولية ورعاية المصابين في حالات الطوارئ، وفرق الاستجابة للكوارث الطبيعية، المعدة للتعامل مع الزلازل

والفيضانات والعواصف. وفي المنشآت الحيوية الكبيرة، قد تُدمج هذه التخصصات في فرق متعددة المهام، أو تُشكل فرق متخصصة لكل نوع من أنواع الطوارئ، بحسب حجم المنشأة وطبيعة المخاطر التي تواجهها."2"

وتتضمن بعض النماذج المعاصرة للاستجابة السريعة تشكيل فرق على المستوى الوطني أو الدولي للتعامل مع تهديدات محددة، كما هو الحال في فرق الاستجابة السيبرانية السريعة (Cyber Rapid Response Teams) التابعة للاتحاد الأوروبي، وهي وحدات متعددة الجنسيات قابلة للنشر السريع لدعم الدول الأعضاء والشركاء في مواجهة الهجمات السيبرانية وحماية البنى التحتية الحيوية، وتعمل هذه الفرق ضمن إطار التعاون الدفاعي الأوروبي المتمثل في التعاون المنظم الدائم (PESCO)، وقد نُشرت فعلياً في أوكرانيا ومولدوفا لدعم حماية الأنظمة الحيوية أثناء فترات حساسة .كما ظهرت مؤخراً نماذج لفرق الاستجابة السريعة للتهديدات الهجينة(Hybrid Rapid Response Teams) ، وهي فرق متعددة التخصصات تُقدم مساعدة سريعة ومصممة خصيصاً لمواجهة حملات التضليل والهجمات السيبرانية والتدخل في الانتخابات، مما يعكس تطور مفهوم الاستجابة السريعة ليشمل أبعاداً أوسع من التهديدات .

ثانياً: تشكيلة فرق الاستجابة السريعة وتوزيع الأدوار

تُبنى فرق الاستجابة السريعة على هيكل تنظيمي واضح يُحدد الأدوار والمسؤوليات بدقة، ويضمن التنسيق الفعال بين الأعضاء أثناء الأزمات. وتشمل التشكيلة النموذجية للفريق قائد الفريق (Team Leader) وهو المسؤول عن القيادة العامة، واتخاذ القرارات، والتنسيق مع غرفة العمليات والإدارة العليا، ونائب القائد الذي يتولى القيادة في غياب القائد ويساعده في إدارة الفريق، وخبراء المجالات المتخصصة كخبراء الحرائق، أو الكيماويات، أو الأمن السيبراني، أو الإنقاذ، وفنيو المعدات المسؤولون عن تشغيل وصيانة المعدات والأجهزة المستخدمة في الاستجابة، ومسؤولو الاتصال المكلفون بالتواصل مع غرفة العمليات والجهات الخارجية، وأفراد الدعم اللوجستي المسؤولون عن توفير المواد والمعدات المطلوبة.

ويُحدد لكل دور متطلباته من التدريب والمهارات والخبرات، وتُوزع المهام بحيث تغطي جميع جوانب الاستجابة المطلوبة، مع تدريب الأفراد على أكثر من دور لضمان التغطية في حال غياب أي منهم. ويُوصى بأن تكون أحجام الفرق متناسبة مع طبيعة المهام، فبعض المهام تتطلب فرقاً صغيرة وسريعة، بينما تتطلب أخرى فرقاً أكبر لتوزيع المهام وتوفير الدعم المتبادل."3"

ثالثاً: التدريب والتأهيل المستمر لفرق الاستجابة السريعة

يُعد التدريب المستمر حجر الزاوية في فعالية فرق الاستجابة السريعة، فالمهارات التي تُكتسب في التدريب هي التي تُميز الفرق الناجحة عن غيرها في لحظات الأزمات الحقيقية. وتشمل برامج التدريب تدريباً أساسياً على الإجراءات والمهارات العامة لجميع أعضاء الفريق، وتدريباً متخصصاً لكل دور في مجالاته المحددة، وتدريبات دورية على سيناريوهات متنوعة تحاكي مختلف أنواع الطوارئ المحتملة، وتدريبات مشتركة مع فرق أخرى داخل المنشأة وخارجها لتعزيز التنسيق، وتدريبات على استخدام المعدات والأجهزة للتأكد من الكفاءة التقنية، وتدريبات على اتخاذ القرارات تحت الضغط والتفكير السريع. ويُوصى بإجراء تمارين مكثفة بشكل دوري، كتمارين شهرية للفرق الصغيرة وتمارين ربع سنوية أو نصف سنوية تشمل المشاركة مع الجهات الأخرى، مع تنويع سيناريوهات التمارين لتشمل حالات نادرة أو غير متوقعة، وتقييم أداء الفرق في التمارين وتقديم تغذية راجعة فورية لتحسين الأداء. وقد أظهرت الدراسات أن الفرق التي تُدرب بانتظام تستجيب بشكل أسرع وأكثر فعالية في الأزمات الحقيقية، وتكون أكثر قدرة على التكيف مع الظروف غير المتوقعة."4"

رابعاً: التجهيزات والمعدات اللازمة لفرق الاستجابة السريعة

تعتمد فرق الاستجابة السريعة في عملها على توفر المعدات والتجهيزات المناسبة في حالة جاهزية دائمة، إذ أن أي نقص أو عطل في المعدات قد يُفقد الفريق القدرة على أداء مهامه في اللحظة الحرجة. وتشمل التجهيزات الأساسية معدات الحماية الشخصية كالخوذ، والسترات الواقية، والأقنعة، والقفازات، والأحذية الخاصة،

وبدلات الحماية من المواد الكيميائية والإشـــعاعية، ومعدات الاتصـــال كأجهزة اللاســلكي والهواتف المؤمنة وأنظمة الاتصـــال عبر الأقمار الصـــناعية، ومعدات الكشـــف والقياس كأجهزة كشـــف الغازات والحرارة والإشـــعاع، ومعدات الإنقاذ والإطفاء كطفايات الحريق، ومعدات القطع والفتح، ومعدات الإنقاذ من الأماكن المرتفعة، ومجموعات الإسعافات الأولية المتقدمة، وأجهزة الكشف عن المتفجرات والمواد الخطرة، ومعدات الدعم اللوجســتي كالإضـــاءة المحمولة ومولدات الطاقة الاحتياطية. وتُخزن هذه المعدات في مواقع استراتيجية قريبة من المناطق المعرضة للخطر، وتُفحص وتُصـــان بشـكل دوري لضـــمان جاهزيتها، مع الاحتفاظ بمعدات احتياطية لتعويض أي أعطال أو استهلاك في المعدات أثناء الاستخدام."5"

خامساً: آلية التنشيط والانتشار السريع للفريق

تُعد آلية تنشـيط الفريق ونشـره من أهم عناصـر نجاح الاسـتجابة السـريعة، إذ أن سـرعة وصـول الفريق إلى موقع الحدث ترتبط مباشـرة بحجم الأضـرار التي يمكن احتواؤها. وتتضمن آلية التنشيط نظام إنذار وتنبيه فوري يصل لأعضاء الفريق عند وقوع أي طارئ، من خلال أجهزة اتصـــال مخصـــصـــة أو تطبيقات طوارئ، وآلية استدعاء سريعة تحدد قنوات وإجراءات استدعاء الفريق في أي وقت، ونظام تحديد موقع ونشـر يوجه أعضـاء الفريق إلى موقع الحدث بأسـرع طريق، وبروتوكولات التنســـيق مع غرفة العمليات لتلقي التوجيهات وتحديث الموقف، وإجراءات الانتقال الآمن إلى موقع الحدث مع تجنب المخاطر الثانوية. ويُوصـى بتحديد أوقات استجابة معيـاريـة لكـل فريق (كـأن يكون الفريق في موقع الحـدث خلال ٥-١٠ دقـائق من التنبيه)، وقياس الأداء الفعلي مقابل هذه المعايير، والعمل على تحسـينها باسـتمرار. وتُجرى تمارين مفاجئة لاختبار ســـرعة التنشـــيط والنشـــر، وتحديد أي عوائق أو تأخيرات في العملية ومعالجتها."6"

سادساً: التنسيق مع غرفة العمليات والجهات الأخرى

لا تعمل فرق الاستجابة السريعة في عزلة، بل تتكامل وتتنسق بشكل وثيق مع غرفة عمليات إدارة الأزمات والجهات الأخرى داخل المنشـــأة وخارجها. ويشـــمل هذا

التنسيق الحفاظ على اتصال مستمر مع غرفة العمليات لتلقي التوجيهات وتحديث المعلومات، والتنسيق مع فرق الاستجابة الأخرى (كفرق الإطفاء والإسعاف) لمنع الازدواجية وتوزيع المهام، والتنسيق مع الجهات الخارجية كالدفاع المدني والشرطة والإسعاف عند الحاجة، والمشاركة في مراكز القيادة المشتركة في الأزمات الكبرى، وتبادل المعلومات حول تطور الموقف والموارد المتاحة. ويُعد التنسيق الفعال بين الفرق المختلفة من عوامل النجاح الحاسمة في إدارة الأزمات، إذ يمنع الفوضى والارتباك، ويضمن استخدام الموارد بكفاءة، ويوفر للجميع صورة موحدة عن الموقف. ويُوصى بإجراء تدريبات مشتركة بانتظام لتعزيز التنسيق، ووضع بروتوكولات واضحة للتواصل والتعاون بين الفرق والجهات المختلفة."7"

سابعاً: إدارة الضغوط النفسية على فرق الاستجابة السريعة

يتعرض أعضاء فرق الاستجابة السريعة لضغوط نفسية كبيرة نتيجة طبيعة عملهم في ظروف خطرة ومضغوطة، مما يستوجب توفير دعم نفسي كافٍ للحفاظ على صحتهم النفسية وكفاءتهم. وتشمل إجراءات الدعم النفسي تدريباً مسبقاً على إدارة الضغوط والتحكم بالانفعالات، وتوفير دعم نفسي فوري بعد الحوادث الكبرى من خلال جلسات تفريغ انفعالي، وإجراء مراجعات دورية للحالة النفسية لأعضاء الفريق، وتوفير فترات راحة كافية بين المهام، وتنويع المهام لتجنب الرتابة والإرهاق، وتوفير بيئة عمل داعمة تشجع على التحدث عن التحديات النفسية دون خوف من الوصم. ويُعد الإرهاق النفسي من أخطر التحديات التي تواجه فرق الاستجابة السريعة، إذ قد يؤدي إلى تراجع الأداء، وزيادة الأخطاء، والإصابات، وارتفاع معدلات التسرب من الفرق، مما يستوجب عناية خاصة من الإدارة وتوفير موارد كافية للدعم النفسي. وقد أظهرت التجارب أن الفرق التي تتلقى دعماً نفسياً منتظماً تكون أكثر استقراراً وأعلى أداءً من تلك التي تُهمل هذا الجانب."8"

ثامناً: تقييم أداء فرق الاستجابة السريعة وتحسينه

تُعد عمليات التقييم والتحسين المستمر جزءاً أساسياً من إدارة فرق الاستجابة السريعة، لضمان بقائها في أعلى مستويات الجاهزية والفعالية. وتشمل هذه العمليات

تقييماً بعد كل حادث حقيقي أو تمرين كبير، يشـــمل تحليل الأداء، وتحديد نقاط القوة والضـعف، واسـتخلاص الدروس المسـتفادة، وتطوير توصـيات تحسـين، وتحديث الإجراءات والتدريبات بناءً على التوصـــيات. وتُســـتخدم في التقييم أدوات متعددة، كتقارير الفريق بعد الحادث، وتحليل التســـجيلات والبيانات، ومقابلات مع أعضـــاء الفريق والجهات المتعاونة، ومقارنة الأداء الفعلي بالمعايير الموضـــوعة. ويُوصـــى بتشجيع ثقافة التعلم المستمر داخل الفرق، حيث يُنظر إلى الأخطاء كفرص للتحسين وليسـت كفشـل، وتُشـارك الدروس المسـتفادة مع الفرق الأخرى لتعميم الفائدة. وتُعد عملية التحســين المســتمر ضــماناً لتطور الفرق واســتمرار قدرتها على مواجهة التحديات الجديدة والمتطورة."9"

وتُشــكل فرق الاســتجابة الســريعة حجر الزاوية في القدرة على التعامل الفعال مع حالات الطوارئ في المنشـــآت الحيوية، فهي الجســـر الذي يربط بين الاســـتعداد النظري والتنفيذ العملي في لحظات الأزمات. وتتطلب هذه الفرق استثماراً متواصلاً في التدريب والتجهيز والدعم النفســـي، وإرادة قيادية تدرك أن تكلفة الإعداد لها أقل بكثير من تكلفة التعامل مع تداعيات عدم الاســـتعداد. وعندما تُبنى وتُدار هذه الفرق بكفاءة، فإنها لا تحمي الأرواح والأصـــول فحســـب، بل تبني ثقافة أمنية متقدمة في المنشأة، وتعزز الثقة بين العاملين والإدارة، وتجعل المنشأة أكثر قدرة على الصمود في وجه أي طارئ، مهما كان حجمه أو تعقيده."10"

التنسيق مع جهات إدارة الأزمات

يُعد التنسيق مع جهات إدارة الأزمات الركيزة التنظيمية التي تحول الاستجابة للطوارئ من جهد منعزل إلى منظومة عمل متكاملة، فهو الحلقة التي تربط إمكانات المنشأة الذاتية بقدرات الجهات الحكومية والأمنية والخدمية، وتضمن استمرارية العمليات الحيوية حتى في أشد الظروف تعقيداً. وتقوم فلسفة هذا التنسيق على مبدأ أن أمن المنشآت الحيوية مسؤولية مشتركة، لا يمكن لأي طرف منفرد أن يضطلع بها بكفاءة، وأن التعاون المسبق والعلاقات المؤسسية القوية بين جميع المعنيين هي التي تحدد غالباً نجاح أو فشل إدارة الأزمات. وقد أثبتت التجارب العملية، كتداعيات الهجوم السيبراني على خط أنابيب كولونيال في عام ٢٠٢١، أن غياب التنسيق الفعال بين القطاعين العام والخاص يمكن أن يحول حادثاً محلياً إلى أزمة إقليمية تمتد آثارها إلى ملايين المواطنين، مما يؤكد أن التنسيق ليس رفاهية تنظيمية، بل ضرورة أمنية وطنية "١"".".4

أولاً: مفهوم التنسيق وأهميته في إدارة الأزمات

يُعرّف التنسيق مع جهات إدارة الأزمات بأنه العملية المنظمة التي يتم من خلالها تبادل المعلومات، وتوحيد الرؤى، وتوزيع المهام، وتكامل الجهود بين المنشأة (بوصفها المالك والمشغل للأصول الحيوية) وجميع الأطراف الخارجية المعنية (كالأجهزة الأمنية، ووكالات الطوارئ، والجهات التنظيمية، والمنشآت المجاورة)، بهدف تحقيق استجابة سريعة وفعالة ومنسقة للطوارئ والأزمات. وتبرز أهمية هذا التنسيق في كونه يمنع الازدواجية وتضارب الجهود، ويضمن الاستخدام الأمثل للموارد المحدودة، ويوفر صورة موحدة ودقيقة عن الموقف لصناع القرار على جميع المستويات، ويسهل الاستفادة من الخبرات والقدرات التخصصية للجهات المختلفة، ويبني الثقة والعلاقات الشخصية التي تُعد حاسمة في لحظات الأزمات. وتشير الدراسات إلى أن التنسيق الفعال يمكن أن يقلل زمن الاستجابة للطوارئ بنسبة تصل إلى ٣٠٪، ويُحسّن جودة القرارات المتخذة في الظروف الحرجة بشكل ملحوظ "٣"".".8

ثانياً: أطراف التنسيق وأدوارهم

يتوزع التنسيق مع جهات إدارة الأزمات على مجموعة واسعة من الأطراف، لكل منها دور محدد يتكامل مع أدوار الآخرين لتشكيل منظومة استجابة شاملة. وتشمل هذه الأطراف، على المستوى المحلي، السلطات المحلية كالبلديات والمحافظات التي تقدم الدعم الخدماتي واللوجستي وتُنسق جهود الإخلاء والإيواء، والأجهزة الأمنية كالشرطة والاستخبارات التي توفر الحماية الأمنية المباشرة والمعلومات الاستخبارية، ووكالات الطوارئ كالدفاع المدني والإسعاف والهلال الأحمر التي تتعامل مع الإطفاء والإنقاذ والإسعافات الأولية، والمنشآت المجاورة التي قد تتشارك في البنى التحتية أو تتأثر بالحوادث نفسها "٣"".10"

وعلى المستوى الوطني، تشمل الأطراف وزارات الدولة كوزارات الدفاع والداخلية والطاقة والصحة، والجهات التنظيمية المسؤولة عن وضع معايير الأمن ومتابعة تنفيذها، ومراكز إدارة الأزمات الوطنية التي تُنسق الاستجابة على المستوى الوطني في حالات الطوارئ الكبرى، وجهات الاستخبارات والأمن الوطني التي تزود بتحليلات التهديدات الاستباقية "١"".١٠". وعلى المستوى الدولي، قد يشمل التنسيق المنظمات الدولية كالوكالة الدولية للطاقة الذرية والمنظمة الدولية للشرطة الجنائية، والدول المجاورة التي قد تتأثر بالحوادث العابرة للحدود، والمنشآت المتعددة الجنسيات التي تعمل عبر الحدود الوطنية "٥"".11"

ثالثاً: آليات التنسيق المؤسسية

تُستخدم آليات متعددة لتفعيل التنسيق بين المنشأة وجهات إدارة الأزمات، تتفاوت في شكلها ودرجة رسميتها، وتشمل لجان التنسيق المشتركة وهي مجالس دائمة تضم ممثلين عن المنشأة والجهات المعنية، تُعقد اجتماعاتها دورياً لمراجعة مستويات التهديد وتحديث خطط الطوارئ ومناقشة التحديات المشتركة. وتُعد الشراكات بين القطاعين العام والخاص (PPP) من أهم هذه الآليات، إذ توفر إطاراً منظماً للتعاون طويل الأمد في مجال حماية البنى التحتية، وقد أظهرت تجارب دولية كتلك التي

طبقتها ولاية ويسكونسن مع شركات الطاقة، أن هذه الشراكات تُعزز بشكل كبير من جاهزية الاستجابة للطوارئ وقدرة التعافي من الأزمات "٣"".6"

وتشمل الآليات أيضاً مراكز العمليات المشتركة التي تُنشأ أثناء الأزمات الكبرى، وتضم ممثلين عن جميع الأطراف المعنية في موقع واحد لتنسيق الجهود وتبادل المعلومات لحظياً، واتفاقيات الدعم المتبادل التي تُبرم مسبقاً بين المنشآت المجاورة أو بين المنشآت والجهات الحكومية، لتحديد كيفية تبادل الموارد والدعم في حالات الطوارئ، وقنوات الاتصال المباشر المتفق عليها مسبقاً، والتي تضمن وصول المعلومة إلى الجهة المناسبة في الوقت المناسب دون عوائق بيروقراطية. وتُعد المشاركة في التمارين والتدريبات المشتركة من أهم آليات بناء التنسيق العملي، إذ تختبر قنوات الاتصال والإجراءات وتُبني الثقة بين الأطراف المختلفة في بيئة آمنة، وقد أشارت توصيات الاتحاد الأوروبي في هذا الصدد إلى أهمية وضع "بروتوكولات زرقاء" للاستجابة للطوارئ، تُحدد بوضوح مسؤوليات كل طرف وتضمن تنسيقاً سلساً أثناء الأزمات "١"".5"

رابعاً: تبادل المعلومات الاستخبارية والتحليلية

يُعد تبادل المعلومات الاستخبارية والتحليلية أحد أهم أوجه التنسيق مع جهات إدارة الأزمات، إذ يُمكّن المنشأة من الاستعداد للتهديدات قبل وقوعها، ويُساعد الجهات الحكومية على فهم تأثير الأزمات على القطاعات الحيوية وتقديم الدعم المناسب. وتشمل المعلومات المتبادلة المعلومات الاستخبارية عن التهديدات المحتملة (كالهجمات الإرهابية أو السيبرانية)، وتحليلات نقاط الضعف في البنى التحتية، وتقارير الحوادث السابقة والدروس المستفادة، وبيانات حالة البنى التحتية الحيوية وتوافر الخدمات، وتقديرات الأثر المحتمل للحوادث على القطاعات المختلفة.

وتُستخدم في تبادل المعلومات منصات آمنة وموثوقة، كمراكز تحليل وتبادل المعلومات (ISACs) المتخصصة في كل قطاع، وأنظمة الإنذار المبكر الوطنية، والاجتماعات التنسيقية الأمنية الدورية. وقد أنشأت الولايات المتحدة مؤخراً تحالفاً وطنياً تحت مسمى ANCHOR-CI يجمع ممثلين عن القطاعين العام والخاص

لتنسيق تبادل المعلومات حول التهديدات ونقاط الضعف، مع توفير بيئة آمنة ومغلقة لمناقشة المعلومات الحساسة، مما يعكس إدراكاً متزايداً بأن التهديدات السيبرانية والفيزيائية المندمجة تتطلب مستوى غير مسبوق من التعاون المعلوماتي بين جميع الأطراف."12"

خامساً: التنسيق أثناء الأزمات (الاستجابة المشتركة)

في لحظة وقوع الأزمة، يتحول التنسيق من كونه نشاطاً تحضيرياً إلى عملية تشغيلية حاسمة، تُحدد فعاليتها مدى نجاح الاستجابة وسرعة التعافي. وتشمل ملامح التنسيق أثناء الأزمات التنشيط الفوري لقنوات الاتصال المتفق عليها مسبقاً، وإبلاغ جميع الأطراف المعنية بطبيعة الأزمة وحجمها والإجراءات المتخذة، وتشكيل مراكز قيادة مشتركة تضم ممثلين عن المنشأة والجهات الحكومية لتوحيد جهود الاستجابة، وتنسيق توزيع الموارد والمعدات والكوادر البشرية بين الأطراف المختلفة، وتبادل المعلومات حول تطورات الموقف بشكل لحظي، وتوحيد الرسائل الإعلامية لتجنب تضارب المعلومات وإرباك الجمهور.

وتتجلى أهمية هذا التنسيق في حالات الأزمات الممتدة أو العابرة للحدود، حيث قد تتطلب جهود الاستجابة تعبئة موارد من عدة دول أو تنسيقاً مع منظمات دولية، وقد وضع الاتحاد الأوروبي "مخططاً أزرق" لتنسيق الاستجابة للاضطرابات العابرة للحدود في البنى التحتية الحيوية، يُحدد آليات تبادل المعلومات وتنسيق الاتصالات العامة والاستجابة السياسية بين الدول الأعضاء، مما يُشكل نموذجاً متقدماً للتنسيق متعدد المستويات في مواجهة التهديدات المعقدة."5"

سادساً: بناء الشراكات وتعزيز الثقة المؤسسية

يُعد بناء الثقة المؤسسية والعلاقات الشخصية بين مسؤولي المنشأة ونظرائهم في جهات إدارة الأزمات من العوامل غير الملموسة ولكنها بالغة الأهمية لنجاح التنسيق. فالعلاقات القائمة على الثقة والاحترام المتبادل تُسهل تدفق المعلومات، وتُسرع عملية اتخاذ القرارات، وتُقلل من البيروقراطية والتردد في لحظات الأزمات. وتُبنى هذه الثقة من خلال اللقاءات الدورية والزيارات المتبادلة،

والمشـــاركة في التمارين والتدريبات المشـــتركة، وتبادل الخبرات والموظفين، والشفافية في التعامل مع الحوادث السابقة والدروس المستفادة.

وتُشـــير التجارب الدولية، كتلك التي وثقتها الوكالة الدولية للطاقة الذرية ومراكز الأمن السيبراني، إلى أن المنشآت التي استثمرت في بناء علاقات وثيقة مع الجهات الحكومية كانت أكثر قدرة على الحصـــول على الدعم الســـريع في الأزمات، وأكثر نجاحاً في تنســـيق جهود التعافي بعد الكوارث. ويُوصـــى بتخصـــيص موارد ووقت كافٍ لبناء هذه العلاقات كجزء من برنامج التجهيز للطوارئ، وعدم اعتبارها نشاطاً ثانوياً أو غير ضروري "٣""٦"".11"

سابعاً: التحديات في التنسيق مع جهات إدارة الأزمات

تُواجه عملية التنســيق مع جهات إدارة الأزمات مجموعة من التحديات التي قد تُعيق فعاليتها، ويتطلب تجاوزها وعياً مسـبقاً وجهوداً متواصـلة. ومن أبرز هذه التحديات اختلاف الثقافات التنظيمية بين القطاع الخاص (الذي يُركّز على الســـرعة والكفاءة والربحية) والقطاع العام (الذي يُركّز على الإجراءات والمســـاءلة والبيروقراطية)، مما قد يؤدي إلى احتكاك وســوء تفاهم في أســاليب العمل وتوقعات الأداء. ويُشــكل تباين مســـتويات الجاهزية والأولويات بين الأطراف المختلفة تحدياً آخر، فقد تكون بعض الجهات أكثر اســـتعداداً واســـتثماراً في مجال إدارة الأزمات من غيرها، مما يُخل بتوازن القدرات في منظومة الاســـتجابة. كما قد تُعيق قيود الســـرية وتبادل المعلومات الحساسة عملية التنسيق، خاصة في المجالات الأمنية والاستخبارية التي تتطلب تصاريح أمنية وإجراءات صارمة قد تُبطئ تدفق المعلومات.

وتُضـــاف إلى ذلك التحديات اللوجســـتية كصـــعوبة التنســـيق بين جهات متعددة ذات ولايات ومســـؤوليات متداخلة، والتباين في الموارد المتاحة بين الأطراف المختلفة، وصعوبة الحفاظ على قنوات الاتصال واستمراريتها في أثناء الأزمات التي قد تُعطل البنى التحتية للاتصـــالات نفســـها. وللتغلب على هذه التحديات، يُوصـــى بتطوير بروتوكولات تنسيق موحدة وواضحة، وإجراء تمارين مشتركة منتظمة، والاستثمار

في أنظمة اتصال احتياطية ومتنوعة، وتعزيز التفاهم المتبادل بين الثقافات التنظيمية المختلفة من خلال برامج تبادل وتدريب مشتركة "١""٦"".8"

ثامناً: التحسين المستمر للتنسيق

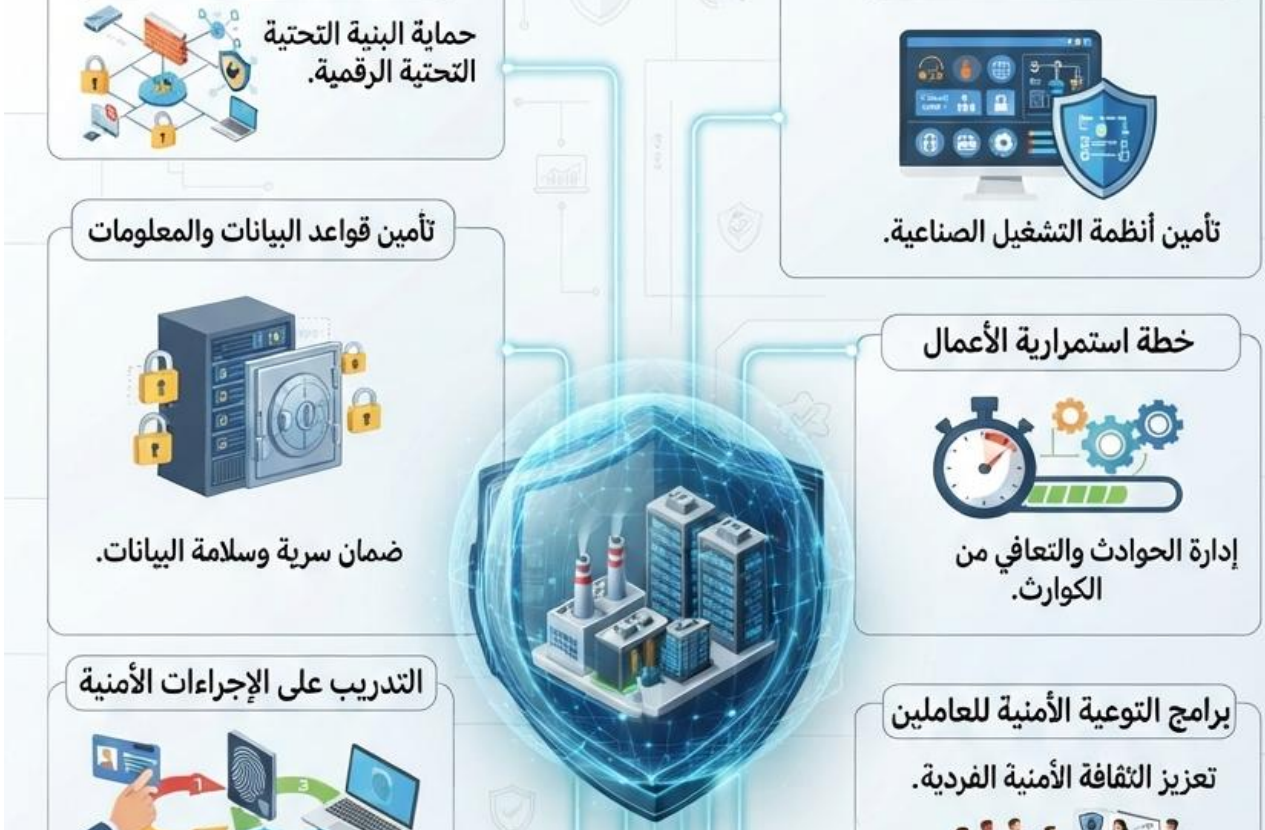
تُعد عملية التنسيق مع جهات إدارة الأزمات نظاماً حياً يتطلب تحديثاً وتحسيناً مستمرين لمواكبة التغيرات في بيئة التهديدات، والتطورات في قدرات الأطراف المختلفة، والدروس المستفادة من الحوادث والتمارين. ويعتمد التحسين المستمر على عدة مصادر، كمراجعة شاملة للتنسيق بعد كل حادث أو تمرين كبير، لتحديد نقاط القوة والضعف ووضع خطط تحسين. وتشمل هذه المصادر أيضاً تحديث خطط الطوارئ والبروتوكولات بالتنسيق مع جميع الأطراف، وإعادة تقييم احتياجات التنسيق في ضوء التغيرات في المنشأة أو البيئة المحيطة، وتطوير آليات جديدة للتعاون وتبادل المعلومات، والاستفادة من الممارسات الفضلى الوطنية والدولية، والاستثمار في التقنيات التي تُسهل التنسيق (كمنصات تبادل المعلومات الآمنة وأنظمة القيادة والسيطرة المتكاملة).

ويُوصى بأن تكون عملية التحسين المستمر للتنسيق جزءاً مدمجاً من برنامج إدارة المخاطر الأمنية في المنشأة، وأن تُخصص لها موارد ومتابعة من الإدارة العليا، وأن تُشرك جميع الأطراف المعنية في عملية التقييم والتطوير لضمان ملاءمة التحسينات للاحتياجات الفعلية. وقد أشارت دراسات التعافي من الكوارث في الأنظمة المتداخلة، كشبكات الطاقة والمياه، إلى أن اعتماد أطر تنسيق تعاونية تكيفية يمكن أن يُحسّن مرونة البنى التحتية بنسبة تصل إلى ٥٪ ويُقلل زمن التعافي بنسبة ٣١٪ مقارنة بالاستراتيجيات غير المنسقة."8"

وتُعد عملية التنسيق مع جهات إدارة الأزمات الاستثمار الأكثر جدوى في مجال الجاهزية الأمنية، فهي تضاعف فعالية الاستثمارات التقنية والبشرية في المنشأة من خلال ربطها بشبكة أوسع من القدرات والخبرات الوطنية، وتحول المنشأة من كيان منعزل يواجه المخاطر بمفرده إلى شريك فاعل في منظومة أمنية وطنية متكاملة. وعندما تُبنى آليات التنسيق وتُدار بكفاءة، فإنها لا تحمي المنشأة فحسب، بل تُسهم

في حماية الأمن القومي واســتقرار المجتمع بأســره، وتُؤكد أن حماية البنى التحتية الحيوية مســؤولية وطنية لا حدود لها، تتطلب تعاوناً وثيقاً بين جميع الأطراف، في السراء والضراء، وفي أوقات السلم والأزمات على حد سواء "١""٣"".12

الوحدة الرابعة:
أمن تقنية المعلومات



حماية أنظمة التحكم الإلكترونية

تأمين أنظمة التشغيل الصناعية.

تأمين شبكات وأنظمة المعلومات

حماية البنية التحتية التحتية الرقمية.

خطة استمرارية الأعمال

إدارة الحوادث والتعافي من الكوارث.

تأمين قواعد البيانات والمعلومات

ضمان سرية وسلامة البيانات.

برامج التوعية الأمنية للعاملين

تعزيز الثقافة الأمنية الفردية.

التدريب على الإجراءات الأمنية

محاكاة وتمارين عملية.

التعاون مع وسائل الإعلام

إدارة الاتصال في الأزمات.

نشر ثقافة اليقظة والتبليغ

تشجيع الإبلاغ عن الحوادث.

مشاركة المجتمع المحلي

إدارة الاتصال في الأزمات الأزمات.

مشاركة المجتمع

التعاون مع المجتمع المحيط.

الوحدة الرابعة: أمن تقنية المعلومات

تمثل هذه الوحدة حجر الزاوية في منظومة الحماية الشاملة للمنشآت الحيوية، حيث تتناول الجوانب التقنية والأمنية المتعلقة بحماية الأنظمة الرقمية والشبكات والبيانات التي تشكل العمود الفقري لتشغيل هذه المنشآت. وتكتسب أهمية خاصة في ظل التحول الرقمي المتسارع وزيادة الترابط بين أنظمة المعلومات وأنظمة التشغيل، مما وسع نطاق الهجمات الإلكترونية وجعلها تهديداً وجودياً للبنى التحتية الوطنية. وتستند منهجية أمن تقنية المعلومات في المنشآت الحيوية إلى فهم عميق للخصائص المميزة لهذه البيئات، حيث تختلف الأولويات اختلافاً جوهرياً عن بيئات تقنية المعلومات التقليدية، إذ تتقدم سلامة الإنسان واستمرارية الخدمة على كل اعتبار آخر.

أولاً: الخصائص المميزة لأمن تقنية المعلومات في المنشآت الحيوية

تتميز متطلبات أمن تقنية المعلومات في المنشآت الحيوية بخصائص فريدة تميزها عن متطلبات الأمن في القطاعات التجارية أو الإدارية التقليدية، وتستند هذه الخصائص إلى طبيعة الأنظمة والعمليات التي تديرها هذه المنشآت. وتبرز في مقدمتها أولوية السلامة والاستمرارية، إذ تتعامل هذه الأنظمة مع عمليات فيزيائية (كشبكات الكهرباء، ومحطات معالجة المياه، والمصانع الكيميائية) حيث قد يؤدي أي فشل أمني إلى كارثة بشرية أو بيئية، مما يجعل السلامة الإنسانية وحماية الأرواح الهدف الأسمى الذي لا يمكن المساومة عليه، كما أن استمرارية الخدمة (Uptime)تمثل أولوية قصوى، وغالباً ما تكون متطلبات التوفر أعلى من متطلبات السرية أو حتى التكامل في كثير من السياقات التشغيلية، فالانقطاع ولو لبضع ساعات قد يكلف الملايين ويعرض حياة المواطنين للخطر.

وتتسم هذه الأنظمة بطبيعة دورة حياة طويلة، إذ تُستخدم المعدات والبرمجيات في أنظمة التحكم الصناعية (OT) لعقود، وقد تستمر بعض الأنظمة في العمل لمدة ٢٠-٣٠ عاماً دون تحديث جوهري، مما يجعلها تحتوي على ثغرات أمنية قديمة ومعروفة، ومن الصعب أو المستحيل تحديثها أو تصحيحها دون تعطيل العمليات.

كما تختلف الأولويات الأمنية بين أنظمة تقنية المعلومات التقليدية وأنظمة التشـغيل، ففي حين تركز أمن المعلومات التقليدي على حماية سـرية البيانات وسـلامتها وتوافرها(CIA) ، تركز أمن أنظمة التشـغيل على السـلامة (Safety) والتوفر (Availability)والموثوقية (Reliability) في المقام الأول، وقد تُضحي السرية من أجل ضمان استمرار العملية التشغيلية.

وتضاف إلى ذلك خصوصية البروتوكولات والمعايير، إذ تستخدم أنظمة التشغيل بروتوكولات اتصال خاصة بالمجال الصناعي كـ (Modbus) و (DNP3) و (PROFINET)، والتي صُممت في الأساس لتحقيق الكفاءة والموثوقية في نقل بيانات التحكم، لا للأمان، وقد تفتقر إلى آليات التشفير أو المصادقة القوية، مما يجعلها عرضة للاستغلال، بينما تكون التهديدات التي تواجهها متطورة ومتنوعة، وتشمل هجمات برامج الفدية، والهجمات السيبرانية المدعومة من دول، والهجمات الداخلية من موظفين أو مقاولين، والهجمات على سلسلة التوريد، والتجسس الصناعي.

ثانياً: فجوة التقارب بين أنظمة تقنية المعلومات وأنظمة التشـغيل (IT/OT Convergence)

يمثل التقارب بين أنظمة تقنية المعلومات وأنظمة التشغيل (IT/OT Convergence)ظاهرة حتمية في سياق التحول الرقمي للمنشآت الحيوية، وهي في الوقت نفسه المصدر الأكبر للمخاطر الأمنية الجديدة. فقد كانت أنظمة التشغيل)كأنظمة التحكم الصناعي (SCADA) وأنظمة التحكم الموزع ((DCS) تعمل في السابق في بيئات معزولة تماماً عن الشبكات الخارجية، مما كان يحد من نطاق التهديدات الإلكترونية. لكن متطلبات الكفاءة والتشغيل عن بُعد والتحليلات المتقدمة والذكاء الاصطناعي فرضت ربط هذه الأنظمة بشبكات المعلومات، مما خلق سطحاً هجوماً ممتداً ومعقداً، وعرّض أنظمة كانت تُصمم بالأساس من أجل السلامة وليس الأمن لمواجهة تهديدات إلكترونية متطورة لم تكن في الحسبان عند تصميمها.

ويكمن التحدي الأســـاســـي في فجوة الثقافة والأولويات بين فرق تقنية المعلومات وفرق التشــغيل، إذ تركز فرق تقنية المعلومات على الســرية والتكامل والتوفر، مع تحديثات وتصــحيحات متكررة للبرمجيات، بينما تركز فرق التشــغيل على الســلامة والتوفر والموثوقية، وتنظر إلى التحديثات والتغييرات على أنها مخاطر تشــغيلية قد تســـبب توقفاً غير مخطط له، كما أن أوقات التوقف المخطط لها نادرة ويصـــعب الحصول عليها.

ولسد هذه الفجوة، تطورت أطر عمل متخصصة تدرك خصوصية بيئات التشغيل، ومن أبرزها المبادئ الستة التي أصدرتها وكالات الأمن السيبراني في دول متعددة (كأستراليا والولايات المتحدة وبريطانيا وكندا وألمانيا وغيرها) بالتعاون المشترك، والتي تقدم إرشادات عملية لتصميم وإدارة بيئات التشغيل (OT) بشكل آمن، وتؤكد على مبادئ أن الســلامة هي الأولوية القصــوى، وأن معرفة الأعمال وفهم الأنظمة التشــغيلية وترابطاتها أمر حاســم لاتخاذ قرارات أمنية ســليمة، وأن بيانات أنظمة التشغيل بالغة القيمة وتستوجب حماية خاصة، مع ضرورة فصل بيئات التشغيل وعزلها عن الشبكات الأخرى، وتأمين سلسلة التوريد، وإدراك أن العنصر البشري هو الركيزة الأساسية لأمن أنظمة التشغيل. وتُعد هذه المبادئ دليلاً عملياً لصناع القرار وللفرق التقنية والإدارية لفهم وتقييم أي قرارات قد تؤثر على أمن بيئات التشغيل، وضمان بقائها آمنة وقادرة على استمرار تقديم الخدمات الحيوية للمجتمع.

ثالثاً: الإطار التنظيمي والتشريعي لأمن تقنية المعلومات في المنشآت الحيوية

يشهد المشهد التنظيمي لأمن تقنية المعلومات في المنشآت الحيوية تطوراً متسارعاً على المســتويين الوطني والدولي، اســتجابة لتصــاعد الهجمات الإلكترونية وتزايد إدراك المخاطر التي تهدد الأمن القومي. وتتنوع هذه الأطر بين معايير تطوعية واشـــتراطات إلزامية تختلف في نطاقها وصـــرامتها بين الدول والقطاعات، لكنها تشترك في هدف تعزيز مرونة البنى التحتية الحيوية ورفع مستوى حمايتها.

ومن أبرز المعايير الدولية المعتمدة في هذا المجال، سلسلة المعايير (ISO/IEC 27001)لإدارة أمن المعلومات، والتي تقدم إطاراً شاملاً لإنشاء وتنفيذ وصيانة

وتحسين نظام إدارة أمن المعلومات(ISMS) ، وتُستخدم على نطاق واسع في مختلف القطاعات بما فيها الطاقة والمياه والاتصالات، وتتضمن متطلبات لتقييم المخاطر، واختيار وتنفيذ الضوابط الأمنية، والمراقبة والمراجعة المستمرة. وقد أصبحت هذه الشهادة في بعض الدول متطلباً قانونياً للمنشآت المصنفة كبنى تحتية حيوية، كما حدث في جورجيا حيث حصل مشغل سوق الكهرباء على الشهادة كجزء من التزامه باللوائح الوطنية ومتطلبات الاندماج مع السوق الأوروبية، مما أسهم في تعزيز إطار الأمن السيبراني وتقليل مخاطر الاختراقات المكلفة كتلك التي تعرض لها في هجوم ببرامج الفدية مطلع عام ٢٠٢٤.

وتُستخدم أطر عمل توجيهية لتقييم وإدارة المخاطر، كإطار الأمن السيبراني الصادر عن المعهد الوطني للمعايير والتقنية (NIST) في الولايات المتحدة، والذي يوفر لغة مشتركة ومنهجية لتحسين إدارة المخاطر السيبرانية، ومناسب لكل من بيئات تقنية المعلومات وأنظمة التشغيل، ويُستخدم على نطاق واسع كممارسة فضلى.

وعلى المستوى الأوروبي، يمثل توجيه أمن الشبكات والمعلومات (NIS-2) نقلة نوعية في التشريع الأوروبي، إذ يُوسع نطاق التطبيق ليشمل عدداً أكبر بكثير من الكيانات (من ٢٠٠٠ إلى حوالي ٣٠٠٠٠)، ويُصنفها إلى فئات "أساسية" و"مهمة" مع متطلبات أمنية وإبلاغ صارمة، ويُلزم الدول الأعضاء بتطبيقه، رغم تأخر بعضها في التنفيذ مما أدى إلى بدء إجراءات مخالفة من المفوضية الأوروبية. كما يهدف مشروع القانون الإطاري الألماني لحماية البنى التحتية الحيوية-KRITIS) (Dachgesetzإلى إدخال متطلبات مستقلة وشاملة للمرونة المادية للبنى التحتية، مما يمثل تحولاً من التركيز على أمن المعلومات وحده إلى نهج شامل يجمع الأمن السيبراني والحماية المادية في إطار واحد متكامل.

وتتضمن بعض التشريعات إجراءات إلزامية محددة، كحظر وصول عناوين (IP) الأجنبية إلى الأنظمة القائمة على الويب التي تديرها البنى التحتية الحيوية، ورفع مستوى حماية المعلومات للجهات الخاصة التي تصل إلى أنظمة المعلومات الحيوية، وتوحيد تسلسل تشغيل الأجهزة الأمنية لتحسين كفاءة الاستجابة، وتشكيل فرق

استجابة للحوادث السيبرانية (SOMEs) وإلزامها بالإبلاغ عن الحوادث للجهات الوطنية المختصة.

رابعاً: آليات الحماية والدفاع السيبراني

تتنوع آليات الحماية والدفاع السيبراني في المنشآت الحيوية لتشمل مجموعة من الضوابط التقنية والإجرائية التي تعمل معاً على مستويات متعددة من الدفاع، وتشكل حواجز متتالية تهدف إلى منع الهجمات، وكشفها، والاستجابة لها، والتعافي من آثارها. وتستند هذه الآليات إلى مبدأ الدفاع المتعمق(Defense in Depth) ، الذي يضمن ألا يؤدي فشل آلية حماية واحدة إلى انهيار المنظومة الأمنية بأكملها.

وتشمل آليات الوقاية والحماية، أنظمة التحكم في الوصول والمصادقة متعددة العوامل (MFA) للتحقق من هويات المستخدمين ومنع الوصول غير المصرح به، وتقييد الامتيازات وتطبيق مبدأ "الحد الأدنى من الصلاحيات"، وحماية الأجهزة الطرفية (Endpoint Protection) باستخدام برامج مكافحة الفيروسات والبرمجيات الخبيثة وأنظمة الكشف والاستجابة للأجهزة(EDR) ، وإدارة الثغرات وتحديث البرمجيات وتصحيحها بانتظام، مع إجراءات اختبار صارمة في بيئات التشغيل قبل التطبيق. وتشمل أيضاً عزل الشبكات وفصل بيئات التشغيل (OT) عن شبكات تقنية المعلومات والشبكات الخارجية باستخدام جدران حماية (Firewalls) ونقاط وصول آمنة، وتأمين الوصول عن بُعد عبر شبكات خاصة افتراضية (VPNs)آمنة ومصادقة مشددة، وتدريب وتوعية العاملين ليكونوا خط دفاع أول ضد هجمات التصيد والهندسة الاجتماعية التي تُعد من أكثر وسائل الاختراق شيوعاً، إذ تشير التقديرات إلى أن ٨٠٪ من الكيانات في القطاعات الحيوية تتعرض لاختراقات أمنية مرتبطة بالبريد الإلكتروني سنوياً بسبب التصيد. وتُعد حماية سلسلة التوريد والتأكد من أمن البرمجيات والمعدات الموردة من البائعين والمقاولين عنصراً حيوياً، إذ يمكن أن تكون هذه السلسلة نقطة ضعف كبيرة، كما حدث في هجمات برمجيات الفدية التي استهدفت أكثر من ٣٠٠ منظمة في القطاعات الحيوية عبر ثغرات في الموردين.

أما آليات الكشف والاستجابة فتشمل أنظمة إدارة المعلومات والأحداث الأمنية (SIEM)وأنظمة كشف ومنع الاختراق (IDS/IPS) لرصد وتحليل الأنشطة المشبوهة واكتشاف محاولات التسلل في الوقت الفعلي، وتطوير خطط استجابة للحوادث تتناسب مع خصوصية بيئات التشغيل، مع إشراك مهندسي العمليات في وضع هذه الخطط وتنفيذها لضمان ألا تؤدي إجراءات الاستجابة إلى تعطيل العمليات الحيوية أو تعريض السلامة للخطر. ويُعد النسخ الاحتياطي للبيانات والأنظمة بشكل منتظم وآمن، مع الاحتفاظ بنسخ غير متصلة بالشبكة (Offline Backups)لضمان القدرة على استعادة الأنظمة بعد الهجمات كتلك التي تستخدم برامج الفدية، عنصراً حيوياً في خطة التعافي.

وتتضمن آليات التقييم والتحسين المستمر، إجراء اختبارات اختراق دورية وتقييمات للثغرات، ومحاكاة هجمات (كتمارين الفريق الأحمر) لتقييم جاهزية الفرق الأمنية وفعالية الضوابط، واستخدام الذكاء الاصطناعي وتعلم الآلة لتحليل كميات هائلة من البيانات وكشف الأنماط الشاذة والتهديدات المتقدمة، مما يُعزز قدرات الكشف المبكر ويُقلل أوقات الاستجابة. وتُظهر الدراسات أن دمج تقنيات الذكاء الاصطناعي في أطر تقييم المخاطر يمكن أن يُحدد احتمالية هجمات متعددة المراحل بدقة قابلة للدفاع، مثل تقدير نسبة نجاح هجوم متقدم على محطة طاقة بنسبة ٨,٧٪، مما يوفر أساساً كمياً للاستثمارات الأمنية الاستراتيجية ويُشكل جسراً للتواصل بين فرق تقنية المعلومات وأنظمة التشغيل والإدارة.

خامساً: التحديات في تطبيق أمن تقنية المعلومات في المنشآت الحيوية

يواجه تطبيق أمن تقنية المعلومات في المنشآت الحيوية مجموعة من التحديات الجوهرية التي تتطلب معالجة دقيقة وواعية، وتتفاوت هذه التحديات بين تقنية وبشرية وتنظيمية، وتستوجب استراتيجيات متخصصة لتجاوزها. ويبرز التحدي الأول في تعقيد بيئات التشغيل (OT) وقدمها، حيث تُستخدم أنظمة قديمة (Legacy Systems)صُممت قبل ظهور التهديدات السيبرانية الحالية، وتعتمد على بروتوكولات اتصال غير آمنة، وتفتقر إلى آليات التشفير والمصادقة الأساسية،

مما يجعل تحديثها أو تصحيحها صعباً أو مستحيلاً دون تعطيل العمليات، وتتطلب حماية هذه الأنظمة حلولاً تعويضية كالعزل الشبكي والمراقبة المستمرة بدلاً من التعديل المباشر.

أما التحدي الثاني فيتمثل في الفجوة الثقافية والتنظيمية بين فرق تقنية المعلومات والتشغيل، إذ تختلف الأولويات والمعايير وطرق العمل بين الفريقين، وقد ينظر مهندسو التشغيل إلى إجراءات الأمن السيبراني على أنها عائق للتشغيل، بينما قد لا يدرك متخصصو تقنية المعلومات الأولويات التشغيلية الحرجة كالسلامة والتوفر، مما يستوجب بناء جسور من التفاهم المشترك وثقافة تعاونية تدمج الأمن في العمليات التشغيلية.

ويُمثل التحدي الثالث نقص الكوادر المؤهلة المتخصصة في أمن أنظمة التشغيل (OT Security)، فهذا المجال يجمع بين معرفة عميقة بأنظمة التحكم الصناعية من جهة وأمن المعلومات من جهة أخرى، وهو مزيج نادر المهارات، مما يجعل توظيف وتدريب الكوادر المناسبة تحدياً كبيراً للمنشآت الحيوية.

ويأتي التحدي الرابع في تزايد وتطور التهديدات السيبرانية، حيث تستخدم الجهات المهاجمة (كالدول والمجموعات الإجرامية المنظمة) موارد كبيرة وتقنيات متطورة كالذكاء الاصطناعي، وتستهدف تحديداً البنى التحتية الحيوية لإحداث أكبر أثر. وقد قدرت التكاليف العالمية المتوسطة لخرق البيانات في عام ٢٠٢٤ بحوالي ٤,٨٨ مليون دولار، وهو رقم يتضاعف بشكل كبير في القطاعات الحيوية نظراً لتأثيراتها المتسلسلة.

وتُضاف إلى ذلك التحديات المتعلقة بسلسلة التوريد، حيث تعتمد المنشآت الحيوية على عدد كبير من البائعين والمقاولين ومقدمي الخدمات، وقد يكون أي منهم نقطة ضعف تسمح باختراق المنشأة، إما عبر برمجيات مخترقة، أو معدات ملوثة، أو حسابات مخترقة، مما يستوجب إدارة صارمة لأمن سلسلة التوريد تمتد لتشمل البائعين والمقاولين أنفسهم.

وتظهر التحديات التنظيمية أيضاً في تعدد الأطر التشريعية وتضاربها أحياناً، إذ قد تخضع المنشأة لقوانين وطنية ومتطلبات قطاعية ومعايير دولية مختلفة، بعضها قد يكون متضارباً أو مكرراً، مما يزيد من عبء الامتثال والتكلفة دون بالضرورة تحسين الأمن الفعلي، كما يظهر في حالة ألمانيا حيث تداخلت متطلبات قطاعية متعددة دون نظام شامل، رغم الجهود لتوحيدها عبر توجيه NIS-2 والقانون الإطاري لحماية البنى التحتية.

وتشكل التحديات المتعلقة بإدارة الأزمات والاستجابة للحوادث تحدياً خاصاً، إذ تتطلب الاستجابة لحادث سيبراني في بيئة تشغيلية تنسيقاً دقيقاً بين فرق تقنية المعلومات والتشغيل والأمن والسلامة والإدارة، وقد تكون إجراءات الاستجابة المعتادة (كإيقاف تشغيل الأنظمة أو قطع الاتصال بالشبكة) غير مقبولة أو خطيرة في بيئة تشغيلية، مما يستوجب خطط استجابة مخصصة وتمارين منتظمة.

وتتطلب مواجهة هذه التحديات استراتيجية متكاملة ومستدامة، تستثمر في الكوادر البشرية، وتطور السياسات والإجراءات، وتدمج الأمن في دورة حياة الأنظمة منذ التصميم، وتتبنى معايير وأطر عمل مرنة قابلة للتكيف، مع إدراك أن أمن تقنية المعلومات في المنشآت الحيوية ليس مشروعاً له نقطة نهاية، بل هو عملية مستمرة من التقييم والتحسين والتكيف مع تطور التهديدات والتقنيات.

تأمين شبكات وأنظمة المعلومات

تُعد شـــبكات وأنظمة المعلومات العمود الفقري الرقمي الذي تقوم عليه عمليات المنشـــآت الحيوية، وتأمينها يمثل تحدياً اســـتراتيجياً متزايد التعقيد، إذ تتداخل فيه متطلبات السلامة التشغيلية مع متطلبات الأمن السيبراني في بيئة تتسم بقدم الأنظمة وتزايد التهديدات. ويقوم تأمين هذه الشبكات على إدراك أن حماية استمرارية الخدمة وسـلامة الأفراد هي الأولويات القصـوى، وأن الإجراءات الأمنية لا يمكن أن تنتقل من ســياقات تقنية المعلومات التقليدية إلى بيئات التشــغيل دون تكييف عميق، نظراً للاختلافات الجوهرية في طبيعة المخاطر والجداول الزمنية للاســـتجابة والثقافات التنظيمية .وتتطلب حماية شـبكات وأنظمة المعلومات في هذه البيئات نهجاً متكاملاً يجمع بين العزل المادي، والمراقبة المسـتمرة، وإدارة المخاطر التكيفية التي تراعي خصوصية كل نظام تشغيلي.

أولاً: التحديات الأساسية في تأمين شبكات وأنظمة المعلومات للمنشآت الحيوية

تتميز بيئات التشـغيل (OT) في المنشـآت الحيوية بخصـائص تجعل تأمينها مختلفاً جوهرياً عن تأمين شـبكات تقنية المعلومات (IT) التقليدية، وتشـكل هذه الخصـائص تحديات تتطلب حلولاً مخصـــصـــة. ويبرز التحدي الأول في طبيعة دورة حياة الأنظمة، إذ تُســتخدم المعدات والبرمجيات في أنظمة التحكم الصــناعية لعقود، وقد تســـتمر بعض الأنظمة في العمل لمدة ٢٠-٣٠ عاماً دون تحديث جوهري، مما يجعلها تحتوي على ثغرات أمنية قديمة ومعروفة، ومن الصـــعب أو المســـتحيل تحديثها أو تصـحيحها دون تعطيل العمليات .في المقابل، يتسـم المجال السـيبراني بالجدة والتطور السريع، حيث تظهر تهديدات وثغرات جديدة بوتيرة أسرع من قدرة الأنظمة القديمة على التكيف، مما يخلق فجوة زمنية بين تطور التهديدات وقدرة الأنظمة على مواجهتها .

ويتمثل التحدي الثاني في التباين الكبير في طبيعة المخاطر بين مجالي تقنية المعلومات والتشغيل، فبينما يركز متخصصو تقنية المعلومات على حماية البيانات والسمعة والإيرادات، يهتم مهندسو التشغيل في المقام الأول بسلامة الإنسان وسلامة

المعدات واستمرارية الخدمات الأساسية .وقد صُممت أنظمة التشغيل في الأساس لتحقيق المرونة المادية والسلامة، ولم يكن الأمن السيبراني مطلباً نموذجياً بسبب ممارسة العزل المادي (Air-Gapping) التي كانت تفصل هذه الأنظمة عن الشبكات غير الآمنة، بينما صُممت أنظمة تقنية المعلومات لتكون مترابطة، مما استلزم الأمن والخصوصية في التصميم والتنظيم .

وتضاف إلى ذلك الفجوة الثقافية والتنظيمية بين فرق تقنية المعلومات والتشغيل، إذ تختلف المسارات المهنية ومتطلبات التعليم والثقافات التنظيمية بين المجالين، فمهندسو التشغيل ينتمون غالباً إلى ثقافة السلامة التي تركز على منع الحوادث غير المقصودة، بينما ينتمي متخصصو تقنية المعلومات إلى ثقافة الابتكار والأمن السيبراني المرتكز على توقع السلوكيات الخبيثة .وقد تؤدي محاولة نقل ممارسات إدارة المخاطر الأمنية مباشرة من مجال السلامة إلى تحديات، لأن الأمن السيبراني يقوم على توقع سلوكيات مستقبلية قد تكون خبيثة، في حين يقوم السلامة على تاريخ معدلات فشل المعدات .

ثانياً: العزل المادي والفصل بين شبكات تقنية المعلومات والتشغيل (IT/OT Segmentation)

يمثل الفصل بين شبكات تقنية المعلومات وشبكات التشغيل أحد أهم الضوابط الأمنية الأساسية لحماية أنظمة التحكم الصناعية، حيث يمنع انتقال التهديدات من بيئات تقنية المعلومات الأكثر عرضة للاختراق إلى بيئات التشغيل الحساسة. وتكتسب هذه الإجراءات أهمية خاصة في ظل تزايد الترابط بين الأنظمة، حيث أصبحت الشبكات المتقاربة تسمح للتهديدات التي تنشأ في بيئات تقنية المعلومات بالانتقال أفقياً إلى أنظمة التشغيل، مما قد يؤدي إلى تعطيل العمليات أو التلاعب بمنطق التحكم أو تعطيل أنظمة السلامة .

وتتفاوت آليات الفصل بين مستويين رئيسيين: مستوى تقليل المخاطر، ومستوى المنع المطلق. ففي المستوى الأول، تُستخدم جدران الحماية وقوائم التحكم في الوصول لتقليل احتمالية الاختراق، لكنها تظل تسمح بالاتصال ثنائي الاتجاه، وتعتمد

على سلامة التهيئة وصيانتها المستمرة، مما يترك مخاطر متبقية .أما المستوى الثاني فيتمثل في المنع المطلق عبر استخدام **موصلات البيانات أحادية الاتجاه (Data Diodes)**، وهي أجهزة أمنية مُطبقة على مستوى العتاد تفرض نقل البيانات في اتجاه واحد فقط، مما يجعل الاتصال العكسي مستحيلاً مادياً، حتى في حال تعرض أنظمة تقنية المعلومات للاختراق الكامل .وتُستخدم هذه الموصلات لنقل بيانات المراقبة والتسجيل من بيئات التشغيل إلى أنظمة التحليل وأقسام أمن المعلومات(Security Operations Centers) ، مع حجب أي محاولة لإرسال أوامر أو تحديثات من الخارج إلى أنظمة التشغيل .

وتُعد المنطقة المنزوعة السلاح الصناعية (Industrial DMZ) حلاً وسطاً يتيح تبادلاً محدوداً ومراقباً للبيانات بين بيئتي تقنية المعلومات والتشغيل، وتوضع فيها الخدمات التي تحتاج إلى اتصال ثنائي الاتجاه مع بيئة التشغيل (كتحديثات البرمجيات أو إدارة الأجهزة)، مع تطبيق ضوابط أمنية مشددة على هذه المنطقة . ويُوصى بتصميم البنى الشبكية وفق نموذج "الدفاع المتعمق Defense in) " (Depth، الذي يجمع بين جدران الحماية، والموصلات أحادية الاتجاه، والمراقبة المستمرة، وإدارة الوصول المقيّد، لضمان ألا يؤدي فشل أي ضابط منفرد إلى انهيار المنظومة الأمنية بأكملها .

ثالثاً: متطلبات الامتثال التنظيمي والتشريعي

يشهد المشهد التنظيمي لتأمين شبكات وأنظمة المعلومات في المنشآت الحيوية تطوراً متسارعاً، استجابة لتصاعد الهجمات الإلكترونية وتزايد إدراك المخاطر التي تهدد الأمن القومي. ويُمثل التوجيه الأوروبي لأمن الشبكات والمعلومات (NIS-2) نقلة نوعية في هذا المجال، حيث يُوسع نطاق التطبيق ليشمل ١٥ قطاعاً (مقارنة بـ ٧ في النسخة السابقة)، ويُصنف الكيانات إلى فئات "أساسية" و"مهمة" مع متطلبات أمنية وإبلاغ صارمة، ويفرض عقوبات مالية كبيرة تصل إلى ١٠ ملايين يورو أو ٢٪ من الإيرادات السنوية العالمية أيهما أعلى للكيانات الأساسية .كما يُلزم التوجيه مجالس الإدارة والمديرين التنفيذيين بالمسؤولية المباشرة عن تدبير المخاطر

السيبرانية والإشراف على الإجراءات الأمنية، وقد تترتب عليهم مسؤولية شخصية في حال ثبوت الإهمال الجسيم بعد حادث سيبراني .

وتشمل المتطلبات الأساسية للتوجيه إجراءات إدارة المخاطر الأمنية التي تشمل إدارة الحوادث السيبرانية، وتعزيز أمن سلسلة التوريد، وتحسين أمن الشبكات، وتطبيق ضوابط وصول وتشفير أفضل، وإعداد خطط لاستمرارية الأعمال تتضمن التعافي من الأنظمة وإجراءات الطوارئ وتشكيل فرق الاستجابة للأزمات .

وتتضمن متطلبات الإبلاغ جداول زمنية محددة، كإرسال "إنذار مبكر" خلال ٢٤ ساعة من اكتشاف الحادث، مما يفرض على المنشآت تطوير قدرات كشف واستجابة سريعة وفعالة .

ويُكمل توجيه NIS-2 توجيه مرونة الكيانات الحيوية (CER) الذي يُركز على المرونة المادية والتشغيلية، ويُشكلان معاً إطاراً تنظيمياً شاملاً يجمع بين الأمن السيبراني والحماية المادية في نهج متكامل لإدارة المخاطر .ومع ذلك، تواجه عملية الامتثال تحديات عملية كبيرة، منها تعقيد تطبيق المتطلبات التنظيمية على أنظمة تشغيل قديمة (Legacy Systems) لم تُصمم مع أخذ الأمن السيبراني في الحسبان، وتجزؤ الحوكمة بين الأطراف المعنية (كمشغلي البنى التحتية، والمقاولين، والموردين، والجهات التنظيمية)، وتفاوت مستويات النضج السيبراني بين الكيانات المختلفة، مما يُعيق التنسيق وتبادل المعلومات، وصعوبة اكتشاف الحوادث والإبلاغ عنها بكفاءة في بيئات التشغيل المعقدة .

رابعاً: آليات الدفاع المتقدم والمراقبة المستمرة

تتطلب طبيعة التهديدات المتطورة التي تواجه شبكات وأنظمة المعلومات في المنشآت الحيوية تطبيق آليات دفاع متقدمة تتجاوز الإجراءات التقليدية، وتستند إلى مبادئ "الثقة المعدومة (Zero Trust) "والمراقبة المستمرة والاستجابة السريعة. وتشمل هذه الآليات أنظمة كشف ومنع التسلل (IDS/IPS) المخصصة لبيئات التشغيل، والتي تراقب حركة البيانات وتحلل الأنماط للكشف عن الأنشطة غير الطبيعية، وأنظمة إدارة المعلومات والأحداث الأمنية (SIEM) التي تجمع وتحلل

السجلات من مصادر متعددة لتوفير رؤية شاملة للتهديدات، وأنظمة الكشف والاستجابة للأجهزة (EDR) التي تراقب السلوكيات المشبوهة على الأجهزة الفردية .

وتكتسب قدرات التحليل المتقدم باستخدام الذكاء الاصطناعي وتعلم الآلة أهمية متزايدة، إذ تتيح تحليل كميات هائلة من البيانات في الوقت الفعلي، وكشف الأنماط الشاذة التي قد تشير إلى هجمات متطورة، وتقديم توصيات للمستجيبين، مما يُعزز القدرة على اكتشاف التهديدات غير المعروفة وتقليل أوقات الاستجابة. وتُستخدم تقنيات المحاكاة واختبارات الاختراق الدورية لتقييم نقاط الضعف في شبكات وأنظمة المعلومات، وتحديد الثغرات التي قد يستغلها المهاجمون، وتطوير إجراءات تصحيحية قبل أن يتم استغلالها في هجمات حقيقية.

وتُعد خطط الاستجابة للحوادث المصممة خصيصاً لبيئات التشغيل عنصراً حيوياً في هذه المنظومة، وتختلف هذه الخطط عن نظيراتها في بيئات تقنية المعلومات التقليدية، إذ يجب أن تراعي خصوصية الأنظمة التشغيلية، وألا تؤدي إجراءات الاستجابة (كإيقاف تشغيل الأنظمة أو قطع الاتصال بالشبكة) إلى تعريض السلامة للخطر أو تعطيل الخدمات الحيوية .وتشمل هذه الخطط إجراءات محددة للتعامل مع مختلف أنواع الحوادث (كالهجمات السيبرانية، وأعطال الأنظمة، والأخطاء البشرية)، وآليات للتواصل مع الجهات الداخلية والخارجية، وإجراءات للتعافي واستعادة الأنظمة، مع إجراء تمارين دورية لاختبار فعالية هذه الخطط وتدريب الفرق على تنفيذها تحت الضغط.

حماية أنظمة التحكم الإلكترونية

تمثل أنظمة التحكم الإلكترونية، والمعروفة أيضاً بأنظمة التشغيل (Operational Technology - OT)، القلب النابض للمنشـــآت الحيوية، فهي المســـؤولة عن مراقبة وإدارة العمليات الفيزيائية كتوليد الكهرباء، ومعالجة المياه، وتشـغيل خطوط الإنتاج، والتحكم في شـــبكات النقل. وتختلف هذه الأنظمة جوهرياً عن أنظمة تقنية المعلومات التقليدية في أهدافها ودورات حياتها ومتطلبات أدائها، حيث تُصـــمم لتحقيق السلامة الفيزيائية والتوفر والموثوقية كأولويات قصوى، وغالباً ما تظل في الخدمة لعقود دون تحديث، مما يجعل حمايتها من الهجمات الســـيبرانية تحدياً معقداً يتطلب منهجيات وأدوات متخصصة "١""٢"".3"

أولاً: الأولويات المختلفة لأنظمة التشغيل

تتبنى أنظمة التشـــغيل نموذجاً أمنياً مختلفاً عن أنظمة تقنية المعلومات، إذ يُعبّر عنه غالباً بـــــ :"AIC" التوفر(Availability) ، والتكامل(Integrity) ، والسـرية (Confidentiality)، على عكس نموذج "CIA" التقليـدي في بيئـات تقنيـة المعلومات. ويُعد التوفر أولوية مطلقة، فالانقطاع غير المخطط له في عمليات توليد الطاقة أو معالجة المياه أو التصنيع قد يتسبب في خسائر فادحة ويُهدد سلامة الأفراد والمجتمع. ويأتي التكامل في المرتبة الثانية، إذ يجب ضـمان عدم التلاعب بالأوامر الصـادرة عن أنظمة التحكم أو البيانات الواردة منها، فالتحكم في سـرعة توربين أو ضـــغط خط أنـابيب يعتمد على ســـلامـة المعلومـات المتبـادلـة بين أجهزة التحكم والمشغلين "٢"".3"

وتختلف الأولويات أيضـــاً في كيفية التعامل مع التحديثات الأمنية، ففي بيئات تقنية المعلومات يُعد تطبيق التصـحيحات بشـكل فوري ممارسـة قياسـية، أما في أنظمة التشـغيل، فإن تحديث البرمجيات أو الأنظمة قد يكون مسـتحيلاً لأن المعدات قديمة ولم تعد مدعومة من قبل الشـركات المصـنعة، أو لأن أخذ النظام الخطير عن العمل لإجراء التحديثات قد يعرض العمليات للخطر، مما يضـطر فرق الأمن إلى الاعتماد على ضوابط تعويضية بديلة."2"

ثانياً: معمارية أنظمة التحكم الإلكترونية

تتكون أنظمة التحكم الإلكترونية في المنشـــآت الحيوية من عدة مكونات رئيســـية تتكامل لتشكل منظومة تحكم متسلسلة. وتشمل هذه المكونات أجهزة التحكم القابلة للبرمجة (PLCs) وهي وحدات تحكم صناعية مسؤولة عن تنفيذ المنطق التشغيلي والتحكم في الأجهزة الميدانية، وأنظمة التحكم الموزعة (DCS) المســـتخدمة في العمليات المستمرة كالمصـافي الكيماوية ومحطات الطاقة، وأنظمة المراقبة والتحكم وجمع البيانات (SCADA) التي تدير البنى التحتية الموزعة جغرافياً كشـــبكات الكهرباء والمياه وخطوط الأنابيب، بالإضـــافة إلى واجهات المشـــغل البشـــري (HMIs)التي تسمح للمشغلين بمراقبة العمليات وإصدار الأوامر "٢""٣". وتشكل هذه المكونات معاً شبكات مترابطة تختلف في بروتوكولاتها وتصميمها عن شبكات تقنية المعلومات، وتستخدم بروتوكولات صناعية متخصصة كـــ Modbus و DNP3وPROFINET ، والتي صُممت في الأساس لتحقيق الكفاءة والموثوقية في نقل بيانات التحكم، وتفتقر غالباً إلى آليات التشـــفير أو المصـــادقة القوية، مما يجعلها عرضـــة للاســـتغلال من قبل المهاجمين الذين يتمكنون من الوصـــول إلى الشبكة."2"

ثالثاً: متطلبات المعايير الدولية لحماية أنظمة التحكم

تُعد سلسلة المعايير (IEC 62443) الإطار المعياري الأكثر شمولاً وقبولاً عالمياً لتأمين أنظمة الأتمتة والتحكم الصناعي(IACS) ، وتغطي جميع مراحل دورة حياة النظام من التصميم إلى التشغيل والصيانة، وتُستخدم كمرجع في العديد من اللوائح التنظيمية للبنى التحتية الحيوية "٤""٥". وتنقســـم الســـلســـلة إلى أربع مجموعات رئيسية: المجموعة العامة التي تتناول المفاهيم الأساسية والمصطلحات، ومجموعة الســـياســـات والإجراءات التي تخص مالكي ومشـــغلي الأنظمة وتتضـــمن متطلبات برنامج الأمن السيبراني، ومجموعة المتطلبات على مستوى النظام التي تشمل تقييم المخاطر وتحديد مستويات الأمن المستهدفة، ومجموعة المتطلبات المتعلقة بتطوير المكونات والمعدات."4"

ويُوصي المعيار بتطبيق نهج "الدفاع المتعمق" في حماية أنظمة التحكم الإلكترونية، وهو نهج طبقي يجمع بين ضوابط متعددة على المستويات المادية والتقنية والإجرائية، بحيث لا يؤدي فشل ضابط منفرد إلى انهيار المنظومة الأمنية بأكملها. ويُعد تقسيم الشبكة إلى مناطق أمنية (Zones) وقنوات اتصال (Conduits) من المبادئ الأساسية للمعيار، حيث تُجمع الأصول المتشابهة في المخاطر والمتطلبات الأمنية في مناطق محددة، وتُحدد قنوات الاتصال الآمنة بينها وفقاً لاحتياجات التشغيل "٤""."5

رابعاً: استراتيجيات الحماية الأساسية

تقوم استراتيجيات حماية أنظمة التحكم الإلكترونية على مجموعة من الممارسات الأساسية التي تُشكل العمود الفقري لأي برنامج أمني في هذا المجال، وتشمل حصر الأصول بشكل كامل ومستمر، إذ لا يمكن حماية ما لا يُرى، ويُعد الحصول على جرد دقيق لجميع الأجهزة المتصلة، بما فيها الأجهزة القديمة وغير المدارة، الخطوة الأولى والأكثر أهمية في أي برنامج أمني، مع اكتشاف جميع مسارات الاتصال المرتبطة بها والعمليات التي تتصل بها "٢""٦". وتشمل أيضاً عزل الشبكات وفصل بيئات التشغيل (OT) عن شبكات تقنية المعلومات والشبكات الخارجية باستخدام جدران حماية ومناطق منزوعة السلاح(DMZ) ، لمنع انتقال التهديدات من بيئات تقنية المعلومات الأكثر عرضة للاختراق إلى أنظمة التشغيل الحساسة، ومنع الحركة الجانبية للمهاجمين في حال اختراق الشبكة عبر التجزئة الدقيقة (Microsegmentation)التي تنشئ مناطق أمنية دقيقة حول الأصول الحيوية "7".

وتشمل الاستراتيجيات الأساسية أيضاً تطبيق مبدأ الامتيازات الدنيا (Least Privilege)والمصادقة متعددة العوامل(MFA) ، لضمان منح المستخدمين والأنظمة والتطبيقات الصلاحيات الضرورية فقط لأداء مهامهم، مع إيلاء اهتمام خاص لتأمين الوصول عن بُعد الذي يُشكل أحد أكثر نقاط الدخول استهدافاً من قبل المهاجمين "٦". وتُعد المراقبة المستمرة للشبكة باستخدام أدوات متخصصة تفهم

البروتوكولات الصناعية، وتحلل حركة البيانات للكشف عن الحالات الشاذة كإرسال أوامر غير معتادة أو غير متوقعة، عنصراً حيوياً في الكشف المبكر عن الهجمات، إلى جانب تطوير استراتيجية رسمية لإدارة التصحيحات تأخذ في الاعتبار الأنظمة التي لا يمكن تحديثها بسهولة، وتستخدم ضوابط تعويضية كالتصحيح الافتراضي وزيادة المراقبة للأصول غير المُحدّثة "٢""."6

خامساً: التهديدات السيبرانية ونواقل الهجوم

تتعرض أنظمة التحكم الإلكترونية لمجموعة متنوعة ومتطورة من التهديدات السيبرانية، التي تتراوح بين الهجمات الإلكترونية المدعومة من دول، وهجمات برامج الفدية، والهجمات الداخلية من موظفين أو مقاولين، وهجمات سلسلة التوريد التي قد تصل عبر برمجيات أو معدات ملوثة "٢""٧". وتتمثل إحدى أخطر نواقل الهجوم في **استخدام المهاجمين لصلاحيات صالحة وأدوات هندسية شرعية** للاندماج في العمليات الطبيعية، مما يجعل اكتشافهم صعباً للغاية، حيث يستخدمون الأدوات نفسها التي يستخدمها مهندسو التشغيل للصيانة والإدارة، ويتحركون ضمن الحدود الطبيعية للنظام."2"

وتشمل نواقل الهجوم الأخرى دخول مورد أو مقاول مصاب ببرمجيات خبيثة عبر توصيل حاسوب محمول أو محرك USB بنظام التحكم، أو تثبيت تصحيحات برمجية أو تحديثات مضادات فيروسات مخترقة. ويُعد نقص الرؤية والأصول غير الموثقة تحدياً كبيراً، إذ وجدت دراسة لأحد المحللين أن ٤٠٪ من المنشآت الصناعية تملك أصولاً متصلة بالإنترنت بشكل غير آمن، وأن ١٢٪ منها كانت تتواصل مع نطاقات خبيثة، مما يزيد بشكل كبير من سطح الهجوم ويعرض الأنظمة للخطر "7".

ويُعد التهديد السيبراني لأنظمة التحكم الإلكترونية في البنى التحتية الحيوية (كشبكات الكهرباء والمياه وخطوط الأنابيب) مصدر قلق استراتيجي على المستوى الوطني، حيث أشارت تقارير حكومية أمريكية إلى أن أنظمة التحكم الإلكتروني للشبكة الكهربائية قد تعرضت لاختراقات متكررة من قبل جواسيس إلكترونيين تابعين لدول

أجنبية، بهدف رسم خريطة النظام وترك برمجيات يمكن استخدامها لتعطيله أو إتلافه في المستقبل، مما يوضح أن التهديدات تتجاوز الجرائم الإلكترونية التقليدية لتشمل أعمالاً عدائية موجهة من دول "٨"".9"

سادساً: اعتبارات إدارة المخاطر والتقييم المستمر

تتطلب حماية أنظمة التحكم الإلكترونية نهجاً منظماً لإدارة المخاطر، يبدأ بتقييم شامل للمخاطر يُحدد التهديدات الواقعية ومسارات الهجوم التي قد تستغلها، بدلاً من الانطلاق مباشرة إلى تطبيق حلول تقنية قد لا تعالج المخاطر الفعلية "٦". وتُستخدم في هذا السياق منهجيات مستمدة من هندسة السلامة كـ Cyber HAZOP و Cyber Bowtieلدراسة وتوثيق التهديدات السيبرانية ونقاط الضعف والعواقب، وتحديد الإجراءات الأكثر فعالية لمنع وتخفيف الحوادث السيبرانية "٢". ويُعد إشراك مهندسي العمليات والمشغلين في ورش عمل تقييم المخاطر أمراً بالغ الأهمية، إذ يمتلكون المعرفة الأعمق بالأنظمة ويفهمونها فهماً قد لا يدركه متخصصو الأمن السيبراني، مما يُمكنهم من تطوير سيناريوهات تهديد واقعية وحلول تخفيف عملية."2"

وتستند عمليات تقييم المخاطر إلى أطر مرجعية كـ MITRE ATT&CK for ICSالذي يوثق التكتيكات والتقنيات التي استخدمها المهاجمون في هجمات حقيقية ضد الأنظمة الصناعية، ويوفر هيكلية لفهم كيفية تحرك المهاجمين في بيئات التشغيل والأدوات التي يستخدمونها، مما يُساعد في تحديد مكان تركيز الضوابط الدفاعية الأكثر فعالية "٢". كما تُستخدم أطر عمل كـ NIST Cybersecurity Framework (CSF)التي توفر لغة مشتركة ومنهجية لإدارة المخاطر السيبرانية، وتركز على خمس وظائف أساسية: التحديد، والحماية، والكشف، والاستجابة، والتعافي "٢"".9"

وتُوصي الممارسات الفضلى باعتماد استراتيجيات قائمة على مبدأ "الثقة المعدومة " (Zero Trust)لتقليل سطح الهجوم ومنع الحركة الجانبية للمهاجمين، حيث يفترض هذا النموذج أن الشبكة معادية في الأساس، وأنه لا يمكن الوثوق بأي جهاز

أو مستخدم بشكل افتراضي، بل يجب التحقق من هويته وصلاحياته في كل مرة يحاول فيها الوصول إلى أي مورد، ويُعد هذا النهج ذا أهمية خاصة في بيئات التشغيل حيث يصعب تحديث الأنظمة القديمة "٧"".10"

تأمين قواعد البيانات والمعلومات

تمثل قواعد البيانات والمعلومات القلب النابض للمنشـــآت الحيوية، فهي المســـتودع المركزي للبيانات التشـغيلية، وسـجلات العملاء، والتصـاميم الهندسـية، والمعلومات الاسـتخبارية، وغيرها من الأصـول غير الملموسـة التي تشـكل قيمة اسـتراتيجية لا تُعوض. ويُعد تعرض هذه البيانات للخطر بمثابة تعريض لأســـرار المنشـــأة وثقة عملائها وميزتها التنافسية، وقد يؤدي تسريبها إلى عواقب وخيمة تمتد من الخسائر المالية إلى الإضرار بالأمن القومي، خاصة في قطاعات الطاقة والمياه والاتصالات. وتقوم استراتيجية تأمين قواعد البيانات على نهج متعدد الطبقات، يدمج بين ضـوابط الوصـــول المشـــددة، وحماية البيانات أثناء التخزين والنقل، والمراقبة المســـتمرة للنشاطات، وإدارة مفاتيح التشفير، مع مراعاة خصوصية بيئات التشغيل ومتطلبات السلامة التي تميز المنشآت الحيوية عن غيرها من البيئات التقنية التقليدية، فلا يمكن تطبيق إجراءات أمن المعلومات القياســـية دون تكييف عميق مع أولويات التشـــغيل والسلامة "٨""."9

أولاً: تصنيف البيانات وتحديد حساسيتها

تُعد عملية تصـــنيف البيانات الخطوة التأســـيســـية والأكثر أهمية في تأمين قواعد البيانات، إذ لا يمكن حماية البيانات بفعالية دون فهم قيمتها ومدى حســـاســـيتها ومتطلبات السرية والتكامل والتوفر الخاصة بكل فئة منها. ويُقسم تصنيف البيانات عادةً في المنشـآت الحيوية إلى عدة مسـتويات، تبدأ بالبيانات العامة التي لا تسـبب أضراراً إذا تسربت، والبيانات الداخلية المخصصة للاستخدام داخل المنشأة والتي قد تسبب ضـرراً محدوداً إذا تسـربت، والبيانات السـرية التي تتطلب حماية مشـددة وقد تسـبب ضـرراً كبيراً إذا تسـربت، والبيانات شـديدة السـرية التي تشـكل خطراً على ســـلامة العمليات أو الأمن القومي إذا تســـربت، مثل بيانات التحكم في شـــبكات الكهرباء، ومخططات المنشـآت النووية، والمعلومات الاسـتخبارية. ويُسـتخدم هذا التصنيف لتحديد الضوابط الأمنية المناسبة لكل فئة، كمتطلبات التشفير، وصلاحيات الوصول، ومدة الاحتفاظ، وإجراءات التدمير الآمن، مع مراعاة أن تصنيف البيانات

ليس عملية لمرة واحدة، بل يتطلب مراجعة وتحديثاً دورياً لمواكبة التغيرات في قيمة البيانات وطبيعة التهديدات "٨"".9"

ثانياً: ضوابط الوصول والمصادقة

تُعد ضـــوابط الوصـــول والمصـــادقة خط الدفاع الأول لحماية قواعد البيانات من الوصـول غير المصـرح به، وتسـتند إلى مبدأ "الحد الأدنى من الصـلاحيات" الذي يمنح كل مستخدم الصـلاحيات الضـرورية فقط لأداء مهامه، ولا أكثر. وتشـمل هذه الضـوابط المصـادقة متعددة العوامل التي تجمع بين عنصـرين أو أكثر من عناصـر التحقق (ككلمة المرور وبصـــمة الإصـــبع أو رمز التحقق)، مما يجعل اختراق الحسابات أمراً بالغ الصعوبة، وإدارة الهوية المركزية التي تُسهل منح الصلاحيات وإلغائها بشكل مركزي وفوري، وتقييد الوصـول إلى الشـبكة باسـتخدام مجموعات الأمان وقوائم التحكم في الوصـول التي تسمح فقط لعناوين (IP) أو تطبيقات محددة بالاتصال بقاعدة البيانات، وتطبيق سياسات كلمات المرور القوية التي تفرض تعقيداً ودورية تغيير مناسـبة لبيئات التشـغيل "١"".١٣". ويُعد الفصـل بين الصـلاحيات الإدارية والتشغيلية من الممارسات الأساسية، بحيث لا يتمتع مسؤولو قواعد البيانات بصـــلاحيات الوصـــول إلى البيانات التشـــغيلية الحســـاســـة، ولا يتمتع المشـــغلون بصلاحيات تغيير هيكل قاعدة البيانات، مما يحد من نطاق الضرر المحتمل في حال اختراق أي من هذه الحسابات."9"

ثالثاً: تشفير البيانات (أثناء التخزين وأثناء النقل)

يُعد تشـفير البيانات ركيزة أسـاسـية في حماية قواعد البيانات، إذ يحول البيانات إلى صـيغة غير مقروءة دون مفتاح فك التشفير، مما يجعلها غير مجدية للمهاجمين حتى لو تمكنوا من الوصـول إليها. ويشـمل التشـفير نوعين رئيسـيين: تشـفير البيانات أثناء التخزين، وهو حماية البيانات المخزنة على وســائط التخزين (كالأقراص الصــلبة) باسـتخدام تقنية التشـفير الشـفاف للبيانات (TDE) التي تشـفر ملفات قاعدة البيانات تلقائياً دون الحاجة إلى تعديل التطبيقات أو اسـتعلامات المسـتخدمين، وتُسـتخدم على نطاق واسـع في المنشـآت الحيوية، مع توصـيات بتدوير مفاتيح التشـفير الرئيسـية

بشكل دوري (ككل ٩٠ يوماً) للحفاظ على أمنها "١""١٣". أما تشفير البيانات أثناء النقل فيهدف إلى حماية البيانات أثناء انتقالها عبر الشبكات بين قواعد البيانات والتطبيقات أو المستخدمين، باستخدام بروتوكولات آمنة كـ(TLS/SSL) ، أو باستخدام ميزات التشفير المدمجة في قواعد البيانات الصناعية، وهو أمر بالغ الأهمية في بيئات التشغيل حيث تنتقل أوامر التحكم والبيانات التشغيلية الحساسة عبر الشبكات "٨""١٣". وتُستخدم في هذا السياق إدارة المفاتيح المركزية كـ (Azure Key Vault)لتخزين وإدارة مفاتيح التشفير بشكل آمن، مع التحكم الدقيق في من يمكنه الوصول إليها، وضمان عدم تخزين المفاتيح مع البيانات المشفرة "٩"".13"

رابعاً: المراقبة والتدقيق المستمر

تتطلب حماية قواعد البيانات في المنشآت الحيوية مراقبة وتدقيقاً مستمرين للنشاطات، لكشف أي محاولات وصول غير مصرح بها، أو أنماط سلوكية شاذة، أو تغييرات غير مبررة في البيانات. وتشمل هذه الإجراءات تسجيل جميع محاولات الوصول إلى قاعدة البيانات (ناجحة كانت أم فاشلة)، مع تسجيل هوية المستخدم، والوقت، ونوع العملية، والبيانات المتأثرة، وتحليل سجلات المراجعة بشكل دوري باستخدام أدوات متخصصة للكشف عن الأنشطة المشبوهة، وإعداد تنبيهات فورية عند حدوث أحداث حرجة (كتغيير صلاحيات، أو محاولات وصول متكررة فاشلة، أو استعلامات غير عادية)، واستخدام أدوات تقييم الأمن الآلية التي تفحص تكوين قاعدة البيانات وتكتشف الثغرات وتُقدم توصيات لمعالجتها "١""٩". وقد أشارت إحدى الدراسات إلى أن تنفيذ البنية الأمنية المتكاملة يمكن أن يحقق أوقات استجابة للتهديدات تقل عن ٥ دقائق، مع ضمان تحديثات أمنية آلية دون توقف، مما يُبرز أهمية الاستثمار في أنظمة المراقبة والتدقيق المتقدمة في بيئات التشغيل الحيوية "9".

خامساً: تأمين النسخ الاحتياطي والتعافي من الكوارث

تُعد النسخ الاحتياطية خط الدفاع الأخير ضد فقدان البيانات أو تلفها، سواء بسبب هجمات برامج الفدية، أو أعطال الأجهزة، أو الكوارث الطبيعية، أو الأخطاء البشرية. وتشمل إجراءات تأمين النسخ الاحتياطي تشفير النسخ الاحتياطية لحمايتها من الوصول غير المصرح به، وتخزين النسخ في مواقع منفصلة ومؤمنة (كموقع احتياطي بعيد) للحماية من الكوارث التي قد تصيب الموقع الرئيسي، واختبار استعادة البيانات بشكل دوري للتأكد من سلامة النسخ وإمكانية استعادتها، وتقييد صلاحيات حذف قواعد البيانات والنسخ الاحتياطية على أقل عدد ممكن من المستخدمين لمنع الحذف المتعمد أو غير المتعمد "١""٩". كما أشارت المبادئ التوجيهية المشتركة من وكالات الأمن السيبراني في عدة دول إلى أهمية فهم متى يمكن الوثوق بالنسخ الاحتياطية بعد حادث سيبراني، خاصة إذا كان المهاجم قد تواجد في الشبكة لفترة طويلة، مما يستوجب تطوير إجراءات للتحقق من سلامة النسخ الاحتياطية واستبعاد احتمال احتوائها على برمجيات خبيثة."8"

سادساً: الاعتبارات الخاصة ببيئات التشغيل(OT)

تختلف متطلبات تأمين قواعد البيانات في بيئات التشغيل) كأنظمة SCADA و DCS) اختلافاً جوهرياً عن بيئات تقنية المعلومات التقليدية، نظراً لأولوية السلامة والتوفر التي تميز هذه البيئات. وتشمل الاعتبارات الخاصة في هذا السياق أن تكون إجراءات الأمن متوافقة مع متطلبات السلامة التشغيلية، بحيث لا تؤدي أي إجراءات أمنية (كتغيير كلمات المرور، أو تحديث البرمجيات، أو تشغيل أدوات التدقيق) إلى تعطيل العمليات الحيوية أو تعريض السلامة للخطر "٨". كما يجب أن يُشرك مهندسو العمليات في تصميم وتنفيذ إجراءات أمن قواعد البيانات، إذ يمتلكون المعرفة الأعمق بالأنظمة والعمليات ويفهمون تأثير أي تغيير أمني على التشغيل والسلامة "٨". ويُعد الحفاظ على توفر البيانات التشغيلية أولوية قصوى، وقد تكون متطلبات التوفر أعلى من متطلبات السرية أو حتى التكامل في كثير من السياقات، فالانقطاع ولو لبضع ساعات قد يكلف الملايين ويعرض حياة المواطنين للخطر، مما

يســتوجب تصــميم حلول أمنية تحقق توازناً دقيقاً بين الحماية واســتمرارية الخدمة "٨"".9

خطة استمرارية الأعمال

تشكل خطة استمرارية الأعمال (Business Continuity Plan - BCP) الإطار الاستراتيجي الذي يضمن للمنشآت الحيوية القدرة على الحفاظ على وظائفها الأساسية أو استعادتها في أقصر وقت ممكن عقب تعرضها لحادث أو كارثة. وتتجاوز هذه الخطة نطاق التعافي التقني لتشمل منظومة متكاملة من الإجراءات البشرية والإدارية والتشغيلية، وهي تختلف جوهرياً عن خطة التعافي من الكوارث (Disaster Recovery Plan - DRP)، فبينما تركز الأخيرة على استعادة البنية التحتية لتقنية المعلومات، تهتم خطة استمرارية الأعمال باستدامة تقديم الخدمات الحيوية للمجتمع، حتى في ظل تشغيل منقوص أو بموارد بديلة. وتكتسب هذه الخطة أهمية استثنائية في سياق المنشآت الحيوية، حيث أن أي انقطاع في خدماتها، سواء كان بسبب هجوم سيبراني، أو كارثة طبيعية، أو فشل في سلسلة التوريد، قد يتسبب في تداعيات متسلسلة تهدد الأمن القومي والسلامة العامة. ويعكس التوجه التنظيمي الحديث، كما ورد في توجيه NIS2 الأوروبي، تحولاً في النظرة إلى استمرارية الأعمال من كونها ممارسة طوعية إلى التزام قانوني، حيث يُلزم الكيانات الحيوية بوضع خطط للاستمرارية تشمل التعافي من الأنظمة وإجراءات الطوارئ، مع إشراف مباشر من مجالس الإدارة .

.1ركائز التخطيط الأساسية (تحليل التأثير وتقييم المخاطر)

ترتكز خطة استمرارية الأعمال الفعالة على فهم عميق للمنشأة ونقاط ضعفها، ويتم ذلك من خلال عمليتين متكاملتين تعتبران حجر الزاوية في التخطيط:

- **تحليل تأثير الأعمال - (Business Impact Analysis BIA):** تهدف هذه العملية إلى تحديد الأنشطة والعمليات الأكثر حساسية واستراتيجية بالنسبة للمنشأة، والتي يجب أن تحظى بأولوية الاستعادة. ويشمل التحليل تحديد الآثار التشغيلية والمالية والقانونية المترتبة على تعطل كل نشاط، وتحديد الفترة الزمنية المسموح بها للتوقف (Recovery Time Objective - RTO)، والحد الأقصى لفقدان البيانات المسموح

به .(Recovery Point Objective - RPO) فعلى سبيل المثال، في منشأة صحية، تكون أنظمة السجلات الإلكترونية للمرضى ذات أولوية قصوى يجب استعادتها خلال ساعات، بينما قد تتحمل الأنظمة الإدارية فترات توقف أطول .

- **تقييم المخاطر :(Risk Assessment)** تقوم هذه العملية بتحديد وتحليل التهديدات المحتملة التي قد تؤدي إلى تعطيل العمليات الحيوية، وتقدير احتمالية حدوثها وحجم تأثيرها. ولا يقتصر نطاق التقييم على التهديدات السيبرانية، بل يشمل الكوارث الطبيعية كالفيضانات والزلازل، وفشل المعدات، وانقطاع التيار الكهربائي، والأزمات الجيوسياسية التي تؤثر على سلاسل التوريد. يساعد هذا التقييم في تحديد السيناريوهات الأكثر ترجيحاً، مما يتيح للمنشأة تطوير استراتيجيات استجابة مخصصة لكل نوع من أنواع الطوارئ .

.2تطوير الاستراتيجيات والخطط

بعد تحديد الأولويات وفهم المخاطر، تنتقل المنشأة إلى مرحلة تطوير الاستراتيجيات العملية التي تضمن استمرار العمل، وتشمل هذه المرحلة ثلاثة محاور رئيسية:

- **استراتيجيات الاستمرارية :**تتضمن وضع حلول بديلة لتجاوز فقدان الموارد الحيوية، مثل: الاتفاق مع موردين بديلين، وتجهيز مواقع عمل احتياطية، واعتماد إجراءات تشغيل يدوية بديلة عن الأنظمة الإلكترونية، وتوزيع الأنظمة الحيوية عبر مراكز بيانات متعددة لضمان التكرار الجغرافي .
- **خطة استمرارية الأعمال :(BCP)** هي الوثيقة التنفيذية التي تفصل الإجراءات الواجب اتباعها خلال الأزمة وبعدها، وتشمل: شروط تفعيل الخطة، وهيكل فرق إدارة الأزمات وأدوار كل فرد، وقنوات الاتصال الداخلية والخارجية، وإجراءات الانتقال إلى وضع التشغيل المنقوص، وخطوات العودة التدريجية إلى العمل الطبيعي .

- **خطة التعافي من الكوارث :(IT DRP)** تُعد جزءاً متخصصاً من منظومة الاستمرارية، وتركز على استعادة أنظمة تقنية المعلومات والبيانات وفقاً للمعايير المحددة في تحليل التأثير RTO) و .(RPOوتشمل إجراءات استعادة البيانات من النسخ الاحتياطية المعزولة Air-gapped) (Backups، وإعادة تهيئة الخوادم، وضمان أمن الشبكات في بيئة ما بعد الحادث .

.3التنفيذ والاعتماد والتدريب

لا تكون الخطة فعالة إلا بتطبيقها على أرض الواقع، مما يستوجب تهيئة البيئة التنظيمية والبشرية لاستقبالها وتنفيذها بكفاءة:

- **الاعتماد والتطبيق :**يجب أن تحظى الخطة بدعم الإدارة العليا، وأن تُعمم على جميع الموظفين، مع حفظ نسخ منها في مواقع بعيدة عن المقر الرئيسي لضمان الوصول إليها في حالات الطوارئ .
- **التدريب والتوعية :**يشمل ذلك تعريف جميع العاملين بأدوارهم ومسؤولياتهم في أثناء الأزمة، وتدريبهم على الإجراءات البديلة، وإجراء تمارين محاكاة دورية (كتمارين الطاولة والمحاكاة الميدانية) لاختبار فعالية الخطة وكشف الثغرات فيها، وهو ما يعد من أفضل الممارسات وفق المعيار الدولي ISO 22301 .

.4المراجعة والصيانة الدورية

نظراً للطبيعة الديناميكية للتهديدات والبيئات التشغيلية، تعد الخطة الحية وثيقة قابلة للتطوير باستمرار:

- **الصيانة والتحديث :**يجب مراجعة الخطة بشكل دوري (سنوياً على الأقل) أو عند حدوث تغييرات جوهرية في البنية التحتية أو القوى العاملة أو نمط التهديدات، وذلك لضمان بقائها ملائمة وفعالة. وتكتسب عملية التدقيق المستقل للخطة ونتائج اختباراتها أهمية خاصة لضمان جودتها .

- **التكامل مع إدارة التغيير :**تُدمج اعتبارات استمرارية الأعمال في عملية إدارة التغيير بالمؤسسة، لضمان أن أي تعديل في الأنظمة أو العمليات يُراجع من منظور تأثيره على قدرة المنشأة على الاستمرار في تقديم خدماتها الحيوية .

برامج التوعية الأمنية للعاملين

تُعد برامج التوعية الأمنية للعاملين حجر الزاوية في أي استراتيجية دفاعية فعالة للمنشآت الحيوية، ذلك أن العنصر البشري، رغم كونه الأصول الأكثر قيمة، يظل الحلقة الأضعف في السلسلة الأمنية، وهو الهدف الأكثر استهدافاً من قبل المهاجمين في العمليات السيبرانية والفيزيائية على حد سواء. وتقوم فلسفة هذه البرامج على مبدأ تحويل العاملين من مجرد مستخدمين للأنظمة إلى خط دفاع أول واعٍ وقادر على التعرف على التهديدات والإبلاغ عنها، وبالتالي تقليص "سطح الهجوم" البشري الذي تستغله هجمات الهندسة الاجتماعية والتصيد الاحتيالي. وتكتسي أهمية خاصة في المنشآت الحيوية نظراً للتأثير الكارثي المحتمل لأي خطأ بشري أو إهمال أمني، حيث وجدت الدراسات أن الخطأ البشري يُعد السبب الجذري لأكثر من ٨٠٪ من الحوادث الأمنية في هذه القطاعات، مما يجعل الاستثمار في التوعية الأمنية ليس رفاهية تنظيمية بل ضرورة أمنية وطنية. وقد تطورت هذه البرامج من مجرد محاضرات توعوية نظرية إلى أنظمة تعليمية تفاعلية، مدعومة بالذكاء الاصطناعي، ومصممة خصيصاً لاستهداف سلوكيات محددة وقياس فعاليتها، مع مراعاة الخصائص الفريدة لكل قطاع من قطاعات البنى التحتية الحيوية.

أولاً: تصميم برنامج التوعية الأمنية

يعتمد تصميم برنامج التوعية الأمنية الفعال على منهجية منهجية تبدأ بفهم عميق للبيئة التنظيمية والمخاطر التي تواجهها، وتشمل عدة مراحل أساسية:

- **تقييم الاحتياجات وتحليل المخاطر :**تُعد هذه المرحلة الأساس الذي يقوم عليه البرنامج، وتبدأ بتقييم شامل للمخاطر الأمنية التي تواجه المنشأة، مع تحديد الفجوات المعرفية والسلوكية لدى العاملين في مختلف المستويات والوظائف.

ويشـــمل هذا التقييم تحليل ســـجلات الحوادث الســـابقة لفهم أنماط الأخطاء البشـرية الأكثر شـيوعاً، وإجراء مقابلات واسـتبيانات لقياس مسـتوى الوعي الأمني الحالي، وتحديد الفئات الأكثر عرضـة للخطر كالعاملين في المناصـب الحساسة أو الجدد، أو أولئك الذين يتعاملون مع معلومات أو أنظمة حساسة، مع إيلاء اهتمام خاص لاختلاف الاحتياجات بين فرق التشغيل (OT) وتقنية المعلومات (IT) نظراً لتباين طبيعة المخاطر والأنظمة التي يتعاملون معها.

- **تحديد الأهداف التعليمية والســـلوكية :**بناءً على تقييم الاحتياجات، تُحدد أهداف تعليمية واضحة وقابلة للقياس لكل مجموعة مستهدفة، ولا تقتصر هذه الأهداف على نقل المعرفة النظرية، بل تمتد إلى تغيير الســـلوكيات وتعزيز الممارسـات الآمنة، مثل: أن يكون الموظف قادراً على التعرف على رسـائل التصـيد الاحتيالي بجميع أشـكالها (بريد إلكتروني، رسـائل نصـية، اتصـالات هاتفية)، وأن يتبع إجراءات الإبلاغ السليمة عند الشك في أي نشـاط مشبوه، وأن يلتزم بسـياســات كلمات المرور والمصـــادقة متعددة العوامل، وأن يفهم العواقب الوخيمة لأي إجراء غير آمن، ليس فقط على المنشـــأة ولكن على سلامة المجتمع والأمن القومي، مع دمج سيناريوهات خاصة ببيئات التشغيل كخطورة توصـــيل أجهزة غير مصـــرح بها بأنظمة التحكم الصـــناعية، أو مخاطر مشاركة معلومات تشغيلية حساسة.
- **تصـميم المحتوى وتنويع الأسـاليب :**يُصـمم المحتوى التعليمي ليكون جذاباً وذا صـلة مباشـرة بمهام العاملين اليومية، مع اسـتخدام مجموعة متنوعة من الأســـاليب التعليمية لمراعاة اختلاف أنماط التعلم، كالمحاضـــرات التفاعلية وورش العمـل، والـدورات الإلكترونيـة (e-learning) التي تتيح التعلم الذاتي، ومقاطع الفيديو والرســوم المتحركة القصــيرة التي تشــرح المفاهيم الأمنية بطريقة مبســطة، والمحاكاة والســيناريوهات التفاعلية التي تضـــع الموظف في موقف حقيقي وتختبر قـدرتـه على اتخـاذ القرار الصـــحيح، والنشـرات الدورية والملصـقات التذكيرية، وألعاب التحدي الأمني. ويُوصـى

بتصـــميم مســـارات تعليمية مخصـــصـــة (Personalized Learning Paths)تتناسـب مع دور كل موظف ومسـتوى المخاطر المرتبط بوظيفته، بدلاً من تقديم محتوى موحد للجميع.

ثانياً: محتوى برنامج التوعية الأمنية

يغطي برنامج التوعية الأمنية الشـامل مجموعة من الموضـوعات الأسـاسـية التي تشـــكل القاعدة المعرفية لكل عامل في المنشـــآت الحيوية، مع تعميق بعض الموضوعات للفئات الأكثر عرضة للخطر:

- **التهديدات السـيبرانية والهندسـة الاجتماعية :**يُعد التوعية بمخاطر الهندسـة الاجتماعية وهجمات التصـــيد الاحتيالي (Phishing) من أهم مكونات البرنامج، وتشـمل تعريف العاملين بأنواع الهجمات المختلفة) كالتصـيد عبر البريد الإلكتروني، والتصيد عبر الرسائل النصية(Smishing) ، والتصيد الصـــوتي(Vishing) ، والهندســـة الاجتماعية عبر وســـائل التواصـــل الاجتماعي(، وتدريبهم على كيفية التعرف على مؤشرات الاحتيال كالعناوين المشـبوهة، والروابط غير المعروفة، والضـغط النفسـي لاتخاذ قرار سـريع، والطلبات غير المعتادة للوصول إلى معلومات حساسة. وتُعد تمارين المحاكاة التفاعلية (Simulated Phishing Campaigns) من أكثر الأدوات فعالية في هذا المجال، حيث يُرسـل للعاملين رسـائل تحاكي هجمات حقيقية، ويُقاس معدل النقر عليها والإبلاغ عنها، وتُســـتخدم النتائج لتوجيه التدريب الإضافي للفئات الأكثر عرضة للخطر.
- **سـياسـات وإجراءات الأمن :**يتضـمن هذا المحور تعريف العاملين بسـياسـات الأمن الداخلي للمنشـأة وإجراءاتها، كسـياسـة الاسـتخدام المقبول، وسـياسـة كلمات المرور والمصادقة متعددة العوامل، وإجراءات التعامل مع المعلومات الحسـاسـة وتصـنيفها، وإجراءات الإبلاغ عن الحوادث الأمنية وعدم معاقبة المبلغين بحسـن نية(No-Blame Culture) ، وسـياسـات أمن الأجهزة المحمولـة والعمـل عن بُعـد، وإجراءات التعـامـل مع الزوار والمقـاولين، مع

التأكيد على أن هذه السياسات ليست قيوداً إدارية بل أدوات لحماية العاملين والمنشأة والمجتمع.

- **الأمن المادي والسلامة :**تشمل التوعية بأمن المحيط والمنشآت، كإجراءات الدخول والخروج، وحماية المعدات والأجهزة من التلف أو السرقة، والإبلاغ عن الأشخاص غير المصرح لهم أو الأنشطة المشبوهة، وإجراءات الإخلاء في حالات الطوارئ، والتعامل مع المواد الخطرة أو المعدات الحساسة.

ثالثاً: قياس الفعالية والتحسين المستمر

لا يمكن لبرنامج التوعية الأمنية أن ينجح دون نظام متكامل لقياس فعاليته وتقييم أثره على السلوكيات والممارسات الأمنية الفعلية، ويشمل ذلك:

- **المؤشرات السلوكية والقابلة للقياس :**قياس التغيير في السلوكيات الأمنية، كمعدل الإبلاغ عن محاولات التصيد، ومعدل الامتثال لسياسات كلمات المرور، ومعدل الإبلاغ عن الأجهزة المفقودة أو المسروقة، وعدد الحوادث الناجمة عن أخطاء بشرية، مع إجراء اختبارات دورية لقياس مستوى المعرفة والمهارات المكتسبة.
- **التغذية الراجعة والاستطلاعات :**جمع آراء العاملين حول جودة المحتوى وطرق التقديم، ومدى ملاءمة البرنامج لاحتياجاتهم، واقتراحاتهم للتحسين، مع تشجيع ثقافة التعلم المستمر، وجعل التوعية الأمنية جزءاً من ثقافة المنشأة وليس مجرد برنامج تدريبي يُختزل في فترة زمنية محددة.
- **الاستفادة من الدروس المستفادة والحوادث :**تحليل الحوادث الأمنية التي وقعت لفهم كيف كان يمكن منعها، وتضمين الدروس المستفادة في محتوى البرنامج، ومشاركة قصص الحوادث الواقعية (مع الحفاظ على السرية) لجعل التوعية أكثر واقعية وتأثيراً.

التدريب على الإجراءات الأمنية

يمثل التدريب على الإجراءات الأمنية الركيزة العملية التي تحوّل السياسات والتوعية النظرية إلى قدرات ميدانية راسخة، فهو المرحلة التي ينتقل فيها العاملون من فهم "ما يجب فعله" إلى التمكن من "كيفية فعله" تحت الضغط وفي ظروف مشابهة للواقع. وتكتسب هذه العملية أهمية خاصة في المنشآت الحيوية، حيث أن أي خطأ في تنفيذ الإجراءات الأمنية، سواء كانت فيزيائية أو سيبرانية، قد يؤدي إلى عواقب كارثية تمتد إلى المجتمع بأكمله. وتختلف برامج التدريب عن برامج التوعية في كونها تركز على اكتساب المهارات العملية والقدرات التشغيلية، وتستهدف فئات محددة من العاملين حسب أدوارهم ومسؤولياتهم الأمنية، مع الاعتماد على أساليب تعليمية تفاعلية ومحاكاة واقعية لسيناريوهات التهديد المحتملة .

أنواع التدريب الأمني ومستوياته

يتنوع التدريب على الإجراءات الأمنية ليشمل عدة مستويات، كل منها يستهدف فئة معينة من العاملين ويحقق أهدافاً تعليمية مختلفة. يبدأ التدريب التأسيسي الإلزامي لجميع العاملين، والذي يغطي الإجراءات الأمنية الأساسية كسياسات الدخول والخروج، وإجراءات الإبلاغ عن الحوادث، والاستجابة للإنذارات، وإجراءات الإخلاء في حالات الطوارئ .ويليه التدريب التخصصي للفئات ذات المهام الأمنية المحددة، كأفراد الأمن المكلفين بتشغيل أنظمة التحكم بالدخول وأجهزة التفتيش، وفرق الاستجابة السريعة، ومشغلي أنظمة التحكم الصناعية، ومسؤولي أمن تقنية المعلومات .أما التدريب المتقدم فيستهدف القادة والمديرين، ويركز على إدارة الأزمات واتخاذ القرارات الاستراتيجية تحت الضغط، والتنسيق مع الجهات الخارجية، وإدارة الموارد في حالات الطوارئ. وقد أشارت الممارسات الدولية، كتلك التي اعتمدتها منظمة الأمن والتعاون في أوروبا (OSCE) في مشروعها PROTECT، إلى أهمية تصميم برامج تدريبية متدرجة تراعي اختلاف الأدوار والمسؤوليات، وتجمع بين التعليم النظري والتمارين العملية الميدانية، لضمان اكتساب المشاركين المهارات اللازمة لتطبيق إجراءات الأمن المادي في منشآتهم،

بدءاً من حماية المحيط وأنظمة كشف التسلل، وصولاً إلى الإضاءة الأمنية وأنظمة التحكم بالدخول .

محتوى التدريب على الإجراءات الأمنية

يغطي التدريب على الإجراءات الأمنية مجموعة من المواضيع الأساسية التي تختلف في عمقها وتفصيلها حسب الفئة المستهدفة. وتشمل المواضيع المشتركة التدريب على إجراءات التحكم في الوصول، كتشغيل أنظمة البطاقات الذكية والقياسات الحيوية، والتحقق من هويات الزوار والمقاولين، وتطبيق إجراءات التفتيش للأفراد والمركبات والبضائع .كما يشمل التدريب على إجراءات المراقبة والرصد، كتشغيل كاميرات المراقبة وأنظمة كشف التسلل، وتحليل الصور والتعرف على السلوكيات المشبوهة، والاستجابة للإنذارات الأمنية. ويُعد التدريب على إجراءات الطوارئ والإخلاء من أهم المكونات، ويشمل تنفيذ خطط الإخلاء بأنواعها (الكلي، الجزئي، الأفقي)، واستخدام مخارج الطوارئ ومعدات الإطفاء، والتعامل مع المصابين وذوي الاحتياجات الخاصة، وممارسة سيناريوهات متنوعة كالحرائق والهجمات الأمنية والكوارث الطبيعية .وتشمل المواضيع المتقدمة التدريب على إجراءات الأمن السيبراني، كتطبيق سياسات كلمات المرور والمصادقة متعددة العوامل، واكتشاف هجمات التصيد والهندسة الاجتماعية والإبلاغ عنها، وتأمين الأجهزة المحمولة والعمل عن بُعد، والاستجابة للاختراقات الإلكترونية في بيئات التشغيل (OT) دون تعطيل العمليات الحيوية .

أساليب التدريب والتقييم

تتنوع أساليب التدريب لضمان تحقيق الأهداف التعليمية بكفاءة، وتشمل المحاضرات النظرية التي تقدم المفاهيم الأساسية والإطار النظري للإجراءات، والعروض التطبيقية التي تشرح تشغيل المعدات والأنظمة الأمنية خطوة بخطوة .وتُعد تمارين المحاكاة والتدريب العملي العنصر الأكثر أهمية، إذ تتيح للمتدربين تطبيق الإجراءات في بيئة تحاكي الواقع، وتشمل تمارين الطاولة (Tabletop Exercises) لمناقشة سيناريوهات الأزمات واختبار فهم الإجراءات، والتمارين

العملية المحدودة كتدريب فرق الإطفاء والإخلاء، والتمارين الشـــاملة التي تشـــمل جميع أقســـام المنشـــأة وتشـــارك فيها جهات خارجية كالدفاع المدني والشـــرطة . وتُستخدم وسائل تقنية متطورة في التدريب، كمنصات المحاكاة الإلكترونية لأنظمة التحكم الصناعية، وأدوات اختبار الاختراق لتقييم جاهزية الفرق السيبرانية، وأجهزة المحاكاة الافتراضية للسيناريوهات المعقدة دون تعريض الأنظمة الحقيقية للخطر . ويشـــمل التقييم اختبارات تحريرية لقياس المعرفة النظرية، وملاحظة الأداء العملي أثناء التمارين، وتحليل القرارات المتخذة في سـيناريوهات المحاكاة، وتقييم سـرعة ودقـة تنفيـذ الإجراءات، مع تقـديم تغـذيـة راجعـة فوريـة للمتـدربين لتعزيز التعلم وتصـــحيح الأخطاء. وقد حددت بعض المعايير المهنية، كتلك المعتمدة في أســتراليا لتطبيق إجراءات حماية البنى التحتية الحيوية، متطلبات أداء واضـحة، تشمل مراقبة أمن منطقة العمل، وجمع المعلومات الاســتخبارية عن التهديدات المحتملة، والتحقق من هوية الأشـخاص والمركبات، وتحديد مؤشـرات النشـاط الإجرامي أو الإرهابي والإبلاغ عنها، وتوثيق تفاصيل التهديدات والاستجابة لها .

•نشر ثقافة اليقظة والتبليغ

نشر ثقافة اليقظة والتبليغ

تمثل ثقافة اليقظة والتبليغ تتويجاً لجهود التوعية والتدريب، فهي الحالة التنظيمية التي يصـــبح فيها الأمن مســـؤولية جماعية، ويتحول فيها كل عامل من مجرد منفذ لإجراءات إلى مراقب يقظ ومشارك فاعل في حماية المنشأة. وتقوم هذه الثقافة على مبدأ أن الأمن ليس مهمة فريق متخصـص فحسـب، بل هو سـلوك يومي يتجسـد في الانتباه للمخالفات، والشعور بالمسؤولية تجاه الإبلاغ عنها، والثقة بأن الإبلاغ سيلقى الاهتمام والسـرية وليس العقاب. وتكتسـب هذه الثقافة أهمية حاسـمة في المنشـآت الحيوية، حيث قد تكون ملاحظة بســيطة من عامل في موقع ما هي الإنذار الوحيد الذي يمنع كارثة وشيكة، فقد أثبتت الدراسات أن برامج الإبلاغ عن المخاطر الفعالة يمكن أن تمنع ما يصـــل إلى ٧٠٪ من الحوادث الأمنية الكبرى في البنى التحتية الحيوية.

عناصر ثقافة اليقظة والتبليغ

تتأســـس ثقافة اليقظة والتبليغ على ثلاثة عناصـــر مترابطة: الوعي، والدافعية، والتمكين. فاليقظة تبدأ بالوعي بما يجب مراقبته، وتســـتمر بالدافعية الذاتية للقيام بـالمراقبة والإبلاغ، وتكتمل بـالتمكين من خلال توفير القنوات الآمنـة والثقة بـأن الإبلاغ ســـيُؤخذ بجدية. ويعني الوعي أن يكون العامل على دراية كافية بأنماط الســـلوك الطبيعي وغير الطبيعي في بيئة عمله، وأن يتمكن من تمييز المؤشـــرات التحذيرية للتهديدات الأمنية، كوجود شخص في منطقة غير مصرح له بها، أو ترك معدات أو حقائب في أماكن غير معتادة، أو محاولة تجاوز الإجراءات الأمنية، أو الحصـول على معلومات حســاســة دون مسـوغ وظيفي، أو رسـائل بريد إلكتروني مشـبوهة، أو تغييرات غير مبررة في سـلوك الزملاء. وتُبنى هذه المعرفة من خلال برامج التوعية المستمرة التي تقدم أمثلة واقعية وحديثة من حوادث وقعت في منشآت مماثلة، وتُظهر بوضوح "شكل الخطر" في سياق العمل اليومي.

أما الدافعية فتنبع من إدراك العامل لأهمية دوره في المنظومة الأمنية، ومن الشـعور بأنه جزء من فريق يحمي زملاءه ومجتمعه، وليس مجرد تابع لإجراءات مفروضـة عليه. ويتطلب بناء هذه الدافعية قيادة أمنية قدوة، تظهر التزامها بـالأمن وتقديرها لجهود العاملين، وتتواصـل باسـتمرار حول أهمية اليقظة والتبليغ، وتشـارك العاملين في النجاحات التي تحققت بفضـــل إبلاغاتهم. ويُعزز ذلك من خلال التكريم المعنوي والمادي للمبلغين، وإبراز قصـص النجاح التي نتجت عن يقظة العاملين (مع الحفاظ على سرية هوياتهم)، مما يخلق تأثيراً مضاعفاً يشجع الآخرين على الاقتداء بهم.

أما التمكين فيتمثل في توفير قنوات إبلاغ متعددة وسـهلة الاسـتخدام وآمنة، كخطوط سـاخنة على مدار السـاعة، وبوابات إلكترونية، وتطبيقات هاتفية، ورسـائل نصـية، وصـــناديق اقتراحات موزعة في مواقع اســـتراتيجية، مع ضـــمان ســـرية المبلغين وحمايتهم من أي انتقام أو تمييز، من خلال تطبيق سياسات عدم الإفصـاح عن هوية المبلغ دون موافقته، ومكافحة أي شـكل من أشـكال الانتقام بحزم، وهو ما يُشـار إليه

أحياناً بثقافة "عدم لوم المبلغ" التي تعد من الممارسات الفضلى في المنشآت عالية الموثوقية.

آليات تعزيز ثقافة اليقظة والتبليغ

لا تُبنى هذه الثقافة بين عشية وضحاها، بل تتطلب استراتيجية متكاملة ومنظمة تعمل على تعزيز السلوكيات المرغوبة وإزالة العوائق التي تثبط الإبلاغ. وتشمل أبرز الآليات الفعالة برامج التوعية التفاعلية المستمرة التي تتجاوز المحاضرات النظرية إلى ورش العمل التي تناقش سيناريوهات حقيقية، وتختبر قدرة العاملين على تحديد السلوكيات المشبوهة، وتحاكي مواقف تتطلب الإبلاغ، وتوضح كيفية القيام بذلك بأمان. كما أن الممارسة الأكثر تأثيراً هي تمارين المحاكاة الميدانية، كأن يُنفذ تمرين مفاجئ لشخص يحاول اختراق منطقة محظورة أو ترك حقيبة مشبوهة، لاختبار مدى يقظة العاملين واستعدادهم للإبلاغ، مع تقديم تغذية راجعة فورية وتعزيز السلوك الإيجابي.

وتُعد السياسات الواضحة والحماية القانونية من الركائز التنظيمية التي تمنح العاملين الثقة اللازمة للإبلاغ، وتشمل سياسة واضحة تحدد آليات الإبلاغ، وتوضح حقوق المبلغين والتزاماتهم، وتؤكد على السرية التامة وحماية المبلغين، مع إجراءات تأديبية رادعة ضد أي انتقام أو تمييز. وقد تضمنت بعض التشريعات الوطنية، كالقانون الأمريكي لحماية البنى التحتية الحيوية، أحكاماً تحمي المبلغين عن المخالفات الأمنية من أي عقاب، مما شجع على الإبلاغ عن ممارسات غير آمنة في قطاعات حساسة كالطاقة والنقل . كما يجب أن تشمل السياسة التزام الإدارة بالتحقيق الجاد في كل بلاغ، وإطلاع المبلغ على نتائج التحقيق (ضمن حدود السرية)، وإغلاق دائرة التغذية الراجعة التي تُعد المحرك الأساسي لاستمرار دافعية الإبلاغ.

دور القيادة في ترسيخ ثقافة اليقظة

يُعد دور القيادة الإدارية العامل الأكثر حسماً في نجاح أو فشل نشر ثقافة اليقظة والتبليغ، فالقيادة هي التي تضع النموذج الذي يحتذى به، وهي التي تُظهر أن الأمن ليس مجرد إجراءات شكلية بل قيمة جوهرية. ويتجلى هذا الدور في التزام الإدارة

العليا بالأمن وتخصيص الموارد الكافية لبرامج اليقظة، وفي الممارسة اليومية لقادة المنشأة كإظهارهم لليقظة بأنفسهم، والإشادة بسلوكيات الإبلاغ، والمشاركة في تدريبات الأمن، والتواصل المنتظم حول أهمية الأمن، وفتح قنوات اتصال مباشرة مع العاملين لتلقي ملاحظاتهم ومخاوفهم الأمنية دون وسطاء، مما يُعزز الثقة ويزيل الحواجز الإدارية.

وتُعد القيادة الأمنية الميدانية، كرؤساء الفرق والمشرفين، الحلقة الأقرب للعاملين اليومية، وهم الأكثر تأثيراً في تشكيل السلوكيات اليومية، لذا يجب تدريبهم على كيفية تعزيز ثقافة اليقظة في فرقهم، وكيفية التعامل مع البلاغات بحساسية واحترافية، وكيفية تشجيع أعضاء فريقهم على الإبلاغ دون ترهيب أو تثبيط. ومن الممارسات الأساسية التي يجب أن تتبناها القيادة مبدأ "الشفافية في التعامل مع البلاغات"، أي إطلاع العاملين على نتائج تحقيقات البلاغات (مع الحفاظ على السرية) ليروا بأعينهم أن بلاغاتهم تُحدث فرقاً حقيقياً، مما يُعزز ثقتهم بالنظام ويحفزهم على الاستمرار في اليقظة والإبلاغ، ويُكمل دورة التغذية الراجعة التي تُعد القلب النابض لثقافة اليقظة المستدامة.

مشاركة المجتمع المحلي في أمن المنشآت الحيوية

تمثل مشـــاركة المجتمع المحلي محوراً اســـتراتيجياً لا غنى عنه في منظومة حماية المنشـآت الحيوية، فهي تنقل الأمن من كونه مسؤولية أجهزة متخصصـة إلى قضـية مجتمعية يتبناها السـكان أنفسـهم. وتقوم فلسـفة هذه المشـاركة على مبدأ أن المنشـآت الحيويـة ليســـت كيانـات معزولـة، بل هي جزء نـابض من النســـيج الاجتمـاعي والاقتصـادي المحيط، وأن سكان المنطقة هم أعين وآذان قادرة على رصد مؤشرات الخطر قبل أن تصل إلى مرحلة متقدمة، مما يجعلهم حجر الزاوية في أي استراتيجية دفـاع وقـائي نـاجح. وقد أثبتت التجـارب العـالميـة أن المجتمعـات المحليـة الواعيـة والمشـاركة تشـكل خط دفاع فعالاً، إذ يمكنها الإبلاغ المبكر عن محاولات التخريب، أو الأنشطة المشبوهة، أو أي تغيرات غير اعتيادية في محيط المنشأة، مما يسهم في تفويت الفرصة على الجهات المعادية ومنع وقوع الحوادث قبل حدوثها.

وتتعدد أشـكال المشـاركة المجتمعية بحسـب طبيعة المنشـأة وخصـائص المجتمع المحيط، وتمتد من بناء الوعي الأمني وصـــولاً إلى المشـــاركة في آليات الرصـــد والإبلاغ. وقد أظهرت الدراسـات الحديثة أن المجتمعات المحلية تشـكل مورداً حيوياً في تعزيز مرونة البنى التحتية، إذ ينظر إليها السـكان كركيزة أسـاسـية لاسـتمرارية الخدمات الحيوية، وفي الوقت نفســه باعتبارها عنصــراً داعماً لاســتقرار الحكومة واسـتمراريتها في حالات الطوارئ، فالمجتمعات المحلية المدركة للخطر والمتعاونة مع الجهات الأمنية قادرة على دعم سـياسـات الأولوية التي تفرضـها الأزمات، حتى لو تطلبت ذلك تحمل تكاليف شخصية مؤقتة.

أولاً: بناء الشراكات مع المجتمع المحلي

يُعد بناء الشراكات المستدامة مع المجتمع المحلي من أهم آليات تعزيز أمن المنشآت الحيوية، إذ يحول العلاقة بين المنشـــأة والمجتمع من علاقة طرفين منفصـــلين إلى شـراكة اسـتراتيجية تقوم على المصـالح المشـتركة والثقة المتبادلة. وتبرز أهمية هذه الشراكات في قدرتها على تحويل السكان من مراقبين سلبيين إلى فاعلين نشطين في منظومة الحماية، مما يخلق شـــعوراً بالملكية والمســـؤولية تجاه المنشـــأة التي تخدم

مجتمعهم. وقد أكدت دراسات عدة أن بناء الشراكات مع المجتمع المحلي يُسهم في تعزيز أمن البنى التحتية الحيوية عبر قنوات متعددة، من أبرزها جمع المعلومات الاستخبارية محلياً والكشف المبكر عن التهديدات، إذ يمتلك السكان المحليون معرفة فريدة بمنطقتهم تمكنهم من ملاحظة الأنشطة غير المعتادة والإبلاغ عنها قبل أن تشكل خطراً على المنشأة. كما أن إشراك المجتمع في جهود الحماية يُعزز الدعم الشعبي للإجراءات الأمنية ويزيد من التعاون مع الجهات الأمنية، مما يُقلل من احتمالية حدوث احتكاكات أو مقاومة قد تعيق تنفيذ الخطط الأمنية.

وتتضمن آليات بناء الشراكات تنظيم لقاءات وحوارات دورية بين مسؤولي المنشأة وقادة المجتمع المحلي (كالعقال، والأئمة، والوجهاء)، لتبادل المعلومات حول التحديات الأمنية المشتركة ومناقشة الحلول، وإنشاء لجان أمنية مشتركة تضم ممثلين عن المنشأة والمجتمع المحلي والجهات الأمنية، تتولى متابعة الوضع الأمني وتنسيق الجهود، وإقامة مشاريع تنموية مشتركة تخدم المجتمع (كالمدارس، والعيادات، ومشاريع المياه)، مما يعزز شعور المجتمع بالارتباط الإيجابي بالمنشأة ويُقلل من احتمالية العداء أو التخريب. وقد أظهرت تجارب شركات النفط والغاز في مناطق الصراع أن الاستثمار في مشاريع تنموية للمجتمع المحلي يُسهم بشكل كبير في تقليل حوادث التخريب وزيادة التعاون الأمني، حيث يبدأ السكان في النظر إلى المنشأة كمصدر للخير وليس كهدف للاستغلال أو التدمير. وتُعد الاتفاقيات الرسمية للشراكة المجتمعية، التي تُحدد التزامات المنشأة تجاه المجتمع وحقوق المجتمع في المشاركة الأمنية، من الأدوات المؤسسية التي تضمن استدامة هذه الشراكات واستمراريتها. وقد تطور هذا المفهوم إلى نماذج متقدمة من الشراكات بين القطاعين العام والخاص (PPP) التي تُدمج المجتمع المحلي كشريك استراتيجي، وتُسهم في تعزيز مرونة البنى التحتية عبر توزيع المسؤوليات وتضافر الجهود بين جميع الأطراف المعنية.

ثانياً: التوعية الأمنية المجتمعية

تُعد التوعية الأمنية المجتمعية الركيزة المعرفية التي تمكن السكان من فهم المخاطر التي تهدد المنشآت الحيوية ودورهم في مواجهتها، وتحولهم من جهلة بالمخاطر إلى مدركين لها قادرين على التعامل معها. وتشمل هذه التوعية برامج إعلامية وتثقيفية تنشرها المنشأة والجهات الأمنية عبر وسائل الإعلام المحلية، ومنصات التواصل الاجتماعي، والنشرات التوعوية، بهدف إطلاع المجتمع على طبيعة المنشأة وأهميتها، والمخاطر التي تتعرض لها، وكيف يمكن للسكان المساهمة في حمايتها. وتشمل آليات التوعية تنظيم محاضرات وورش عمل في المدارس والمراكز الثقافية لتعريف الأجيال الناشئة بأهمية المنشآت الحيوية ودورهم المستقبلي في حمايتها، وإطلاق حملات توعوية في وسائل الإعلام المحلية تركز على عواقب التخريب والإضرار بالمنشآت الحيوية، والأضرار التي تلحق بالمجتمع بأكمله عند تعطل هذه المنشآت، إلى جانب نشر خطوط ساخنة وقنوات إبلاغ سهلة الاستخدام، وتعريف المجتمع بكيفية استخدامها للإبلاغ عن أي أنشطة مشبوهة.

ولم تقتصر فعالية التوعية المجتمعية على الجانب النظري، بل امتدت إلى تحقيق نتائج ملموسة في مجالات عدة، منها تعزيز الوعي بمخاطر التخريب، حيث أظهرت إحدى الدراسات في أوغندا أن حملات التوعية الوطنية ساهمت في زيادة الإبلاغ عن حوادث تخريب البنية التحتية للكهرباء، حيث بات السكان يدركون أن هذه الجريمة ليست بلا ضحية، بل هي عمل مميت يعرض الأرواح للخطر ويعيق التنمية الوطنية. كما أنها أدت إلى تحفيز السلوك الاستباقي، حيث أصبح السكان أكثر ميلاً للإبلاغ عن الأنشطة المشبوهة واعتبار حماية البنية التحتية مسؤولية مشتركة بين جميع أفراد المجتمع، مما حوّل المجتمعات المحلية من مراقبين سلبيين إلى عيون وآذان أمنية تسهم في حماية المنشآت الحيوية التي تخدمها وتدعم استقرار الدولة.

ثالثاً: آليات الإبلاغ المجتمعي والتغذية الراجعة

تُعد آليات الإبلاغ المجتمعي الفعالة الجسر الذي يربط بين وعي المجتمع وقدرته على العمل، إذ تتيح للسكان نقل ملاحظاتهم ومعلوماتهم بشكل سريع وآمن إلى الجهات المعنية، مما يُحول اليقظة المجتمعية إلى إجراءات عملية. وتشمل هذه الآليات خطوط ساخنة تعمل على مدار الساعة لتلقي البلاغات من المجتمع، وتطبيقات هاتفية سهلة الاستخدام تسمح بإرسال صور ومواقع الحوادث بدقة، وصناديق اقتراحات وإبلاغ موزعة في الأماكن العامة، مع ضمان سرية المبلغين وحمايتهم من أي انتقام، وتوفير مكافآت تشجيعية للمبلغين عن معلومات تؤدي إلى كشف تهديدات أو منع حوادث. وقد أثبتت التجارب الميدانية في دول عدة أن أنظمة الإبلاغ المجتمعي أسهمت بشكل فعال في كشف شبكات سرقة النفط والغاز، وضبط عصابات التخريب في قطاع الكهرباء والاتصالات، مما أدى إلى خفض معدلات الحوادث الأمنية بشكل ملحوظ. وتُعد آلية التغذية الراجعة جزءاً لا يتجزأ من نجاح نظام الإبلاغ، إذ يجب إطلاع المجتمع على نتائج بلاغاته، ليشعر بأن مساهمته مؤثرة ومُقدَّرة، مما يعزز دافعيتهم للاستمرار في اليقظة والإبلاغ، ويُكمل الدورة التفاعلية التي تبني الثقة بين المجتمع والجهات الأمنية والمنشأة.

وتشمل آليات الإبلاغ المتقدمة أنظمة الإنذار المبكر المجتمعية التي تربط السكان مباشرة بغرف العمليات، وتسمح بنقل المعلومات الاستخبارية المحلية بسرعة فائقة، وقد أظهرت تجربة مدينة همدان الإيرانية في إجراء تمرين "الاعتماد على الذات في الأحياء" عام ٢٠٢٥، حيث تم تفعيل نظام اتصال بدائي عبر الإنترنت (تطبيق روبيكا) بين مركز العمليات وقادة ٧٠ حياً، وفي مرحلة لاحقة عندما تم فرض سيناريو انقطاع الاتصالات، انتقلت التقارير عبر سعاة بالدراجات النارية، مما يُظهر أهمية وجود قنوات اتصال بديلة ومرنة لضمان استمرارية التنسيق بين المجتمع والجهات الأمنية حتى في أسوأ الظروف.

رابعاً: تعزيز الانتماء والمواطنة الأمنية

تتجاوز مشـاركة المجتمع المحلي في أمن المنشـآت الحيوية الجانب العملي إلى بناء منظومة قيمية تعزز الانتماء والمواطنة الأمنية، حيث يشعر كل فرد بأن حماية البنية التحتيـة واجـب وطني وليس مجرد إجراء أمني. وتُبنى هذه القيم من خلال غرس مفـاهيم المواطنـة الأمنيـة في المنـاهج التعليميـة وبرامج الإعلام الموجهـة للأطفـال والناشـــئة، لتشـــكيل وعي مبكر بأهمية المنشـــآت الحيوية ودور الفرد في حمايتها. وتشمل برامج تعزيز الانتماء تنظيم فعاليات مجتمعية مشتركة بين المنشأة والمجتمع المحلي، كالأيام المفتوحة التي تتيح للســـكان زيارة المنشـــأة والتعرف على طبيعة عملها وأهميتها، والمشـاركة في حملات التطوع لتنظيف المحيط أو صـيانة المرافق العامة المرتبطة بالمنشـأة، مما يعزز الشـعور بالملكية المشـتركة، وإطلاق مبادرات تحفيزية تكرم الأفراد والمجموعات التي تسـهم في حماية المنشـآت الحيوية، سـواء عبر الإبلاغ عن مخاطر، أو المشـــاركة في فعاليات توعوية، أو أي شـــكل آخر من أشكال التعاون الأمني.

وتُعد الشـراكة مع المؤسـسـات الدينية والثقافية والمجتمع المدني من الأدوات المؤثرة في ترسـيخ قيم المواطنة الأمنية، حيث يمكن لهذه المؤسـسـات نشـر رسـائل توعوية موجهـة لفئـات مجتمعيـة محـددة، ونقل قيم حمـايـة الممتلكـات العـامـة والبنيـة التحتيـة كجزء من الواجـب الـديني والأخلاقي والاجتمـاعي. وقـد أظهرت تجـارب جهـات حكومية كالوكالة الوطنية للتوجيه في نيجيريا فعالية إشراك القيادات التقليدية والدينية في حملات التوعية بحماية البنى التحتية، مما ساهم في تغيير نظرة المجتمع إلى هذه المنشآت من أصول حكومية غريبة إلى ممتلكات وطنية تستوجب الحماية والمحافظة عليها من التخريب والعبث.

وتشـــكل مشـــاركة المجتمع المحلي ركيزة لا غنى عنها في منظومة أمن المنشـــآت الحيوية، فهي تحول الأمن من مهمة أمنية متخصـصـــة إلى قيمة مجتمعية راسـخة، وتســـتثمر المعرفة المحلية والقدرات المجتمعية في خدمة الحماية الوقائية. وعندما تُبنى هذه المشـاركة على أسـس سـليمة من الوعي والثقة والشـراكة، فإنها لا تحمي

المنشآت فحسب، بل تعزز التماسك الاجتماعي، وتدعم التنمية المستدامة، وتُرسخ مبدأ أن أمن الدولة هو مسؤولية الجميع، وأن حماية البنى التحتية ليست مجرد إجراء أمني، بل هي استثمار في مستقبل الأجيال القادمة واستقرار الوطن.

التعاون مع وسائل الإعلام في أمن المنشآت الحيوية

يمثل التعاون مع وسائل الإعلام ركيزة استراتيجية لا غنى عنها في منظومة حماية المنشآت الحيوية، فهو الجسر الذي يربط بين الجهات الأمنية والمجتمع، ويُعد أداة فاعلة في تشكيل الوعي العام، وتعزيز الأمن الوطني الشامل، ومكافحة الشائعات والمعلومات المضللة التي قد تهدد استقرار المنشآت وسلامة المجتمع .وتقوم فلسفة هذا التعاون على إدراك أن وسائل الإعلام ليست مجرد ناقل للأخبار، بل هي شريك أساسي في صون الاستقرار، من خلال تعزيز الوعي الوطني، وتوسيع دائرة المشاركة المجتمعية، وبناء الثقة المتبادلة بين المؤسسات الرسمية والجمهور .وقد حظي هذا المفهوم باهتمام متزايد على المستويين الوطني والدولي، حيث أُدرجت وسائل الإعلام العامة في بعض التصنيفات كبنية تحتية حيوية، نظراً لدورها المحوري في دعم الديمقراطية والتماسك الاجتماعي، وتوفير معلومات دقيقة تعمل كحاجز ضد انتشار "الأخبار الزائفة"، مما يجعل أداءها الصحي مهماً لأمن المجتمعات واستقرارها .

دور وسائل الإعلام في تعزيز الأمن الوطني

تُعد وسائل الإعلام أداة مزدوجة التأثير، إذ يمكن استخدامها كسلاح للدم destruction، أو أداة للمعلومات، أو وسيلة للدفاع، مما يجعل دورها في الأمن الوطني بالغ الحساسية والتأثير .وتتجلى مسؤولية الإعلام في هذا السياق من خلال عدة وظائف رئيسية، أبرزها نشر الوعي الأمني، حيث تقدم وسائل الإعلام معلومات دقيقة وفي الوقت المناسب للجمهور، مما يعزز الوعي بتهديدات الأمن القومي، ويحول الجمهور إلى عنصر يقظ ومسؤول قادر على التصرف بشكل استباقي .كما تلعب دوراً محورياً في تشكيل التصورات العامة، فعندما تقدم وسائل الإعلام روايات صادقة ومتوازنة، فإنها تمكن الجمهور من الانخراط في نقاشات مستنيرة، وتعزز التماسك الوطني، خاصة في أوقات الأزمات أو جهود المصالحة .

وتتولى وسائل الإعلام مسؤولية مكافحة الشائعات والمعلومات المضللة، التي تُعد من أخطر التهديدات التي تواجه المجتمعات الحديثة، إذ يمكن أن تخلق الارتباك

وتقوض الثقة في المؤسسات، وتقوض الأمن الوطني، كما حدث في بعض النزاعات المسلحة التي تحول فيها الصحفيون إلى دعاة للدعاية .وقد أبرزت توجيهات رسمية في الأردن وكينيا أهمية الإعلام المسؤول في التصدي للدعاية الموجهة، وصياغة رواية وطنية موحدة تعزز قدرات الدولة وتدعم الجبهة الداخلية، مع ضرورة التحقق الدقيق من المصـــادر وتجنب التكهن والاعتماد على أدلة موثوقة للحفاظ على ثقة الجمهور .وتشير المناقشات في محافل متخصصة، كمنتدى مكافحة الإرهاب في كينيا، إلى أن الإعلام غير المســؤول والمنحاز يمكن أن يدعم أهداف الجماعات الإرهابية، بينما يُعد الالتزام بالمعايير الأخلاقية ركيزة أساسية لضمان أن يسهم العمل الإعلامي بشكل إيجابي في مكافحة التطرف العنيف .

بناء شراكات استراتيجية بين القطاع الأمني والإعلامي

يتطلب التعاون الفعال مع وسائل الإعلام بناء شراكات استراتيجية مؤسسية تتجاوز العلاقات الظرفية، وتقوم على أسس من الثقة المتبادلة، والتدريب المشترك، وتبادل الخبرات. وقد تجسد هذا التوجه في العديد من المبادرات الدولية والوطنية، ففي قطر مثلاً، وقعت الوكالة الوطنية للأمن الســيبراني مذكرة تفاهم مع مجموعة "بي إن ميديا" بهدف تعزيز التعاون في مجالات التوعية الأمنية وبناء القدرات الوطنية، وتشمل تقديم فرص تدريبية لموظفي المجموعة في برامج متخصصة، والمشاركة في ورش عمل وجلسات توعوية، والتعاون في إنتاج محتوى توعوي، ونشر حملات التوعية عبر المنصات الإعلامية للوصول إلى فئات أوسع من المجتمع .وتُظهر هذه الشراكة إدراكاً بأن التوعية والتدريب يشكلان خط الدفاع الأول ضد التهديدات الســيبرانية، وأن الاســتثمار في ثقافة أمنية قوية لا يقل أهمية عن الاســتثمار في التقنيات المتقدمة .

وعلى صعيد مشابه، أطلقت منظمة "مركز أفريقيا للتحول الرقمي" في غانا مشروعاً وطنياً بالشــراكة مع هيئة الأمن الســيبراني، يهدف إلى تعزيز المعرفة الأمنية لدى العاملين في وسائل الإعلام المجتمعية، وتزويدهم بمهارات عملية للتعامل مع قضايا الأمن السيبراني، ومكافحة التضليل، وتعزيز السلامة الرقمية، والإبلاغ عن البنى

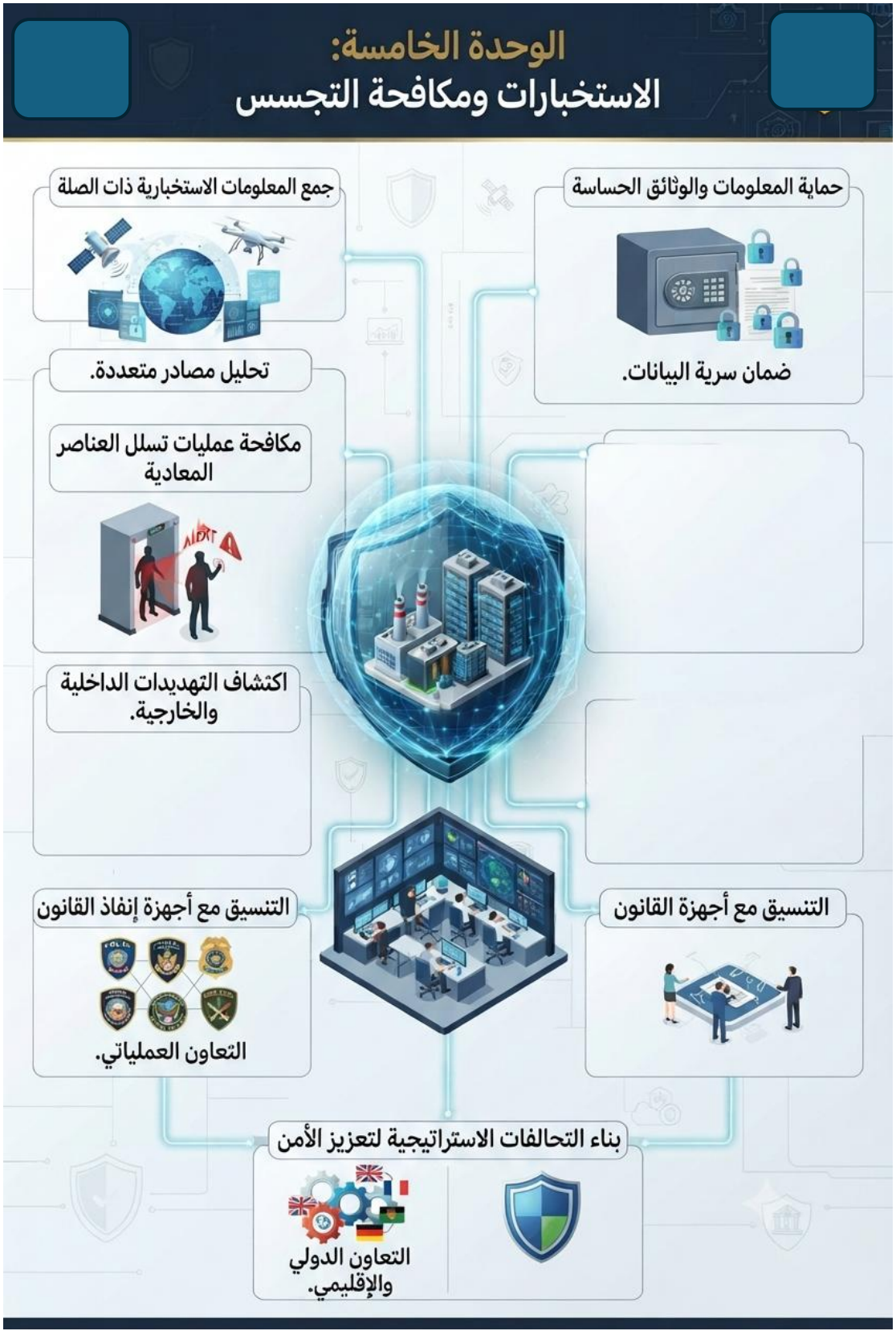
التحتية الحيوية للمعلومات، وتعزيز المرونة السـيبرانية في مجتمعاتهم .ويشـمل المشـروع تدريباً مكثفاً للصـحفيين، يتبع ذلك منحهم شـهادة وإدماجهم في "فيلق الصحافة الأمنية"، وهو شبكة وطنية من المهنيين مكرسة لتعزيز التوعية الأمنية من خلال الصحافة المسؤولة، مما يُعد نموذجاً تطبيقياً لتحويل الإعلام إلى شريك فاعل في منظومة الأمن الوطني .

الاعتبارات الأخلاقية والتوازن بين الأمن وحقوق الجمهور

يمثل التعاون مع وسائل الإعلام في المجال الأمني عملية موازنة دقيقة بين ضرورة حماية الأمن القومي من جهة، وحق الجمهور في المعرفة وحرية التعبير من جهة أخرى، وهو ما يثير مجموعة من الاعتبارات الأخلاقية والقانونية. وتتمثل إحدى أهم هذه الاعتبارات في ضـرورة الالتزام بالمهنية والموضـوعية، وتجنب الإثارة والتحيز، والتحقق الدقيق من المعلومات قبل نشـرها، لأن التقارير غير الدقيقة قد تُضـلل الجمهور، وتُصـعّد التوترات، وتُغذي الروايات المتطرفة، وتُقوض الأمن الوطني .كما يجب أن يراعي الإعلام حساسية المعلومات المتعلقة بالأمن القومي، فلا يمكن نشـر كل المعلومات، إذ توجد مواد مصـنفة ذات أهمية وطنية، وقد يؤدي سعي الإعلام للحصول على بعضها إلى الإضرار بالأمن القومي .

وتبرز هنا الحاجة إلى تطوير خطاب إعلامي أمني وعسـكري متخصـص، يتميز باحترافية عالية، ويوازن بين تزويد الجمهور بالمعلومة وحماية الأمن الوطني، مع خطط تواصل مدروسة للتعامل مع الشائعات والمعلومات المضللة، وترسيخ ثقافة إعلامية مسؤولة تحترم الخصوصية والحرية مع الحفاظ على المصلحة الوطنية العليا .وتلعب المؤسسات الأكاديمية والبحثية دوراً في هذا السياق من خلال دراسة سـبل تعزيز التعاون بين الإعلام والأجهزة الأمنية، وتقديم توصـيات لتطوير أطر تنظيمية وأخلاقية تضمن استمرار هذا التعاون في إطار من المسؤولية والشفافية .

الوحدة الخامسة:
الاستخبارات ومكافحة التجسس



الوحدة الخامسة: الاستخبارات ومكافحة التجسس

تمثل الاستخبارات ومكافحة التجسس الركيزة الاستباقية في منظومة حماية المنشآت الحيوية، فهي تنتقل بالأمن من التفاعل مع التهديدات إلى توقعها واستباقها، ومن الدفاع السلبي إلى العمل الهجومي الاستباقي. وتقوم فلسفة هذا المجال على إدراك أن التهديدات الموجهة للبنى التحتية الوطنية لم تعد مقتصرة على الهجمات المباشرة، بل تشمل شبكة معقدة من أنشطة التجسس، والاختراقات السيبرانية الممتدة، والعمليات الخفية التي تهدف إلى استنزاف القدرات الوطنية والتأثير في القرارات الاستراتيجية. وقد توسع نطاق عمل مكافحة التجسس بشكل كبير في العقود الأخيرة، متجاوزاً حماية الأسرار العسكرية والدبلوماسية ليشمل حماية الملكية الفكرية، والتكنولوجيا الحيوية، والبيانات التشغيلية للبنى التحتية، وسلاسل التوريد، وسلامة الفضاء المعلوماتي "٦". وقد أشارت دراسات حديثة إلى أن التهديدات السيبرانية والإرهاب البيئي، بأشكالهما غير المتماثلة، باتت تشكل تحدياً متزايداً يتطلب استجابة استخباراتية ومضادة للتجسس متكاملة واستراتيجية."1"

أولاً: تطور مفهوم الاستخبارات الأمنية في حماية البنى التحتية

شهد مفهوم الاستخبارات الأمنية للمنشآت الحيوية تحولاً جوهرياً من نهج تفاعلي قائم على جمع المعلومات عن التهديدات المعروفة، إلى نهج استباقي يقوم على التنبؤ بالتهديدات وتحليل نوايا الخصوم وقدراتهم قبل أن تتحقق. ويعكس هذا التطور التغير في طبيعة التهديدات نفسها، فلم تعد مقتصرة على عمليات التجسس التقليدية، بل توسعت لتشمل هجمات سيبرانية متطورة، وحملات تضليل إعلامي، وعمليات تخريبية مدعومة من دول، وأنشطة إرهابية بيئية تستهدف البنى التحتية "١""٦". وتقوم الاستخبارات الأمنية الفعالة على مبدأ "الاستخبارات المبنية على التهديد " (Threat-Driven Intelligence)، حيث تُصمم أنشطة جمع المعلومات وتحليلها بناءً على فهم دقيق للجهات المهددة وأساليبها وأهدافها، بدلاً من جمع المعلومات بشكل عشوائي. وقد أظهرت النماذج العملية، كتلك المطبقة من قبل وزارة الأمن الداخلي الأمريكية، فعالية دمج ضباط الاستخبارات مع مستشاري

الأمن الوقائي في مراكز الدمج (Fusion Centers) على مستوى الولايات، لتوفير رؤية محلية وإقليمية للمخاطر تدعم الصورة الوطنية للتهديدات."5"

وتشمل الاستخبارات الأمنية متعددة المصادر دمج معلومات من مصادر متنوعة، كالاستخبارات مفتوحة المصدر(OSINT) ، والاستخبارات السيبرانية، والاستخبارات البشرية، وتحليلات وسائل التواصل الاجتماعي، لبناء صورة شاملة ودقيقة عن بيئة التهديدات. وقد زادت أهمية الاستخبارات مفتوحة المصدر بشكل كبير مع انتشار منصات التواصل الاجتماعي والمواقع الإلكترونية، حيث أصبحت تشكل مصدراً غنياً للمعلومات عن نوايا الخصوم وأنشطتهم، مما يستوجب تطوير قدرات تحليلية متخصصة للاستفادة منها "٢". كما تبرز أهمية الاستخبارات التنافسية (Competitive Intelligence) في القطاع الخاص، التي تركز على فهم تحركات المنافسين والجهات المعادية في السوق، وحماية الميزة التنافسية من خلال كشف محاولات التجسس الصناعي وسرقة الأسرار التجارية."6"

ثانياً: مكافحة التجسس في بيئة التهديدات المعاصرة

تُعد مكافحة التجسس (Counterintelligence) الركيزة الدفاعية في مواجهة جهود الدول والجماعات المعادية لجمع المعلومات عن المنشآت الحيوية أو الإضرار بها. وتوسع نطاق مكافحة التجسس بشكل كبير ليشمل ثلاثة أبعاد رئيسية: حماية الأسرار التقنية والتكنولوجية، وحماية البنى التحتية المادية والرقمية، وحماية الفضاء المعلوماتي من عمليات التضليل والتأثير "٦". ويتمثل التحدي الأكبر في بيئة مكافحة التجسس المعاصرة في استهداف الخصوم لسلاسل التوريد، حيث يسعون لإدخال "أبواب خلفية" أو إنشاء "نقاط اختناق" قابلة للاستغلال في مراحل التصنيع أو التوزيع، مما يستوجب ممارسات صارمة للعناية الواجبة (Due Diligence)عبر سلسلة التوريد بأكملها."6"

وتكتسب مكافحة التجسس أهمية خاصة في قطاعات التكنولوجيا المتقدمة، حيث تسعى الدول للتفوق التقني عبر سرقة الملكية الفكرية والأسرار التجارية، وهو ما يُعد تهديداً استراتيجياً قد يغير موازين القوى العالمية. وقد أشارت تحليلات إلى أن

الفشل في دمج الذكاء الاصطناعي بشكل استراتيجي في منهجيات مكافحة التجسس قد يؤدي إلى تآكل منهجي للميزة التكنولوجية والاقتصادية الوطنية "٦". ويشمل عمل مكافحة التجسس أيضاً حماية المعلومات من التسرب عبر القنوات البشرية، من خلال تطبيق إجراءات الفحص الأمني للموظفين، وتقييد الوصول إلى المعلومات الحساسة، ومراقبة الأنشطة المشبوهة، وتدريب العاملين على التعرف على محاولات التجسس والإبلاغ عنها."6"

ثالثاً: الاستخبارات السيبرانية وحماية أنظمة التشغيل

تُعد الاستخبارات السيبرانية (Cyber Intelligence) ركيزة حيوية في حماية أنظمة التشغيل (OT) والبنى التحتية الحيوية، إذ تركز على جمع وتحليل المعلومات حول التهديدات السيبرانية التي تستهدف هذه الأنظمة، وتوفير رؤى استباقية تمكن من التصدي للهجمات قبل وقوعها. وتشمل الاستخبارات السيبرانية مراقبة شبكات الاتصالات، وتحليل حركة البيانات، وكشف الأنماط الشاذة التي قد تشير إلى اختراق أو استعداد لهجوم "٢""٧". وتُستخدم أدوات متطورة في هذا المجال، كأنظمة إدارة المعلومات والأحداث الأمنية(SIEM) ، ومنصات تحليل التهديدات المدعومة بالذكاء الاصطناعي، التي تتيح معالجة كميات هائلة من البيانات في الوقت الفعلي واكتشاف التهديدات المتقدمة التي قد تفوت الأنظمة التقليدية "٧"."11"

وتبرز أهمية الاستخبارات السيبرانية بشكل خاص في مواجهة التهديدات المستمرة المتقدمة(APTs) ، التي تتميز بطول أمدها وصعوبة اكتشافها، إذ تستخدم أساليب متطورة للبقاء داخل الشبكات لفترات طويلة دون أن تُكتشف، بهدف جمع المعلومات أو التمركز لشن هجمات مستقبلية. وتشمل أنشطة الاستخبارات السيبرانية تحليل هجمات القرصنة السابقة لفهم تكتيكات المهاجمين وتقنياتهم وإجراءاتهم، ومشاركة المعلومات الاستخبارية مع مراكز تحليل وتبادل المعلومات القطاعية(ISACs) ، والجهات الحكومية، والمنشآت الأخرى "٩". ويُعد دمج الاستخبارات السيبرانية مع الاستخبارات المادية خطوة متقدمة في حماية البنى التحتية، إذ تتيح ربط التهديدات

الرقمية بالآثار المادية المحتملة، وتوفير صـورة شـاملة للمخاطر التي تدمج البعدين السيبراني والفيزيائي في تقييم موحد "٢"."9"

رابعاً: تحديات تطبيق الاستخبارات ومكافحة التجسس في المنشآت الحيوية

تواجه تطبيقات الاسـتخبارات ومكافحة التجسـس في المنشـآت الحيوية مجموعة من التحديات العملية التي تتطلب وعياً واســـتراتيجيات لتجاوزها. ويبرز التحدي الأول في صـــعوبة التنســـيق بين القطاعين العام والخاص، إذ تختلف الأولويات والثقافات التنظيمية، وتُقيد قيود الســـرية تبادل المعلومات، مما قد يُعيق تدفق الاســـتخبارات الحيوية بين الجهات المختلفة "١". وتشـير الدراسـات إلى أن التحديات في التنسـيق بين القطاعات واستمرار الحاجة لتطوير الأطر التشغيلية والتنظيمية على المستويين الوطني والدولي تشكل عقبات كبيرة أمام حماية فعالة للبنى التحتية."1"

ويُشـــكل نقص الكوادر المؤهلة تحدياً آخر، فمجال الاســـتخبارات الأمنية ومكافحة التجســـس يتطلب مزيجاً نادراً من المهارات التحليلية والتقنية والأمنية، مما يجعل توظيف وتدريب الكوادر المناســـبة صـــعباً ومكلفاً، وقد تتطلب بعض المهام الاستخباراتية تصـاريح أمنية عالية لا تتوفر بسـهولة في القطاع الخاص "٢""١٠". ويُضـــاف إلى ذلك تطور التهديدات بوتيرة أســـرع من قدرة الأنظمة الدفاعية على التكيف، خاصـــة في مجالات الذكاء الاصـــطناعي والتعلم الآلي، حيث يســـتخدم الخصوم هذه التقنيات لأتمتة عمليات التجسس وتحليل كميات هائلة من البيانات، مما يستوجب مواكبة دفاعية مماثلة "٦"."7"

وتُعد حماية سـرية عمليات الاسـتخبارات ومكافحة التجسـس تحدياً في حد ذاتها، إذ يجب أن تجمع المعلومات وتحللها دون الكشـف عن مصـادرها أو أسـاليبها، مما قد يُعيق التعاون مع الشـــركاء ويُحد من نطاق المشـــاركة في التبادل الاســـتخباراتي. ويتطلب ذلك بنية تحتية أمنية مشددة، وعمليات تشغيلية سرية، وثقافة تنظيمية تحافظ على السرية دون أن تعيق فعالية العمليات، خاصـة في حالات الطوارئ التي تتطلب سرعة في اتخاذ القرارات "٦"."10"

حماية المعلومات والوثائق الحساسة

تمثل حماية المعلومات والوثائق الحساسة أحد الركائز الجوهرية في منظومة الاستخبارات ومكافحة التجسس، إذ تشكل هذه المعلومات الهدف الأول لعمليات التجسس والاختراقات، سواء من قبل دول معادية، أو جماعات إجرامية، أو حتى منافسين في القطاع الخاص. وتتجاوز هذه الحماية مجرد وضع كلمات مرور أو أقفال على الملفات، لتشمل منظومة متكاملة من السياسات والإجراءات والضوابط التقنية والمادية التي تضمن سرية المعلومات وتكاملها وتوفرها، وفق نموذج "CIA"المعدل ليتناسب مع أولويات المنشآت الحيوية حيث يتقدم التوفر أحياناً على السرية، خاصة في البيانات التشغيلية لأنظمة التحكم الصناعي "٢""١٥". وتستند استراتيجية حماية المعلومات الحساسة إلى فهم دقيق لطبيعة هذه المعلومات، وتصنيفها وفق درجة حساسيتها، وتطبيق ضوابط متناسبة مع كل فئة، مع مراعاة المتطلبات القانونية والتنظيمية التي تفرضها التشريعات الوطنية والدولية.

أولاً: تصنيف المعلومات وتحديد حساسيتها

تُعد عملية تصنيف المعلومات الخطوة التأسيسية والأكثر حسماً في حماية المعلومات الحساسة، إذ لا يمكن حماية ما لا يُعرف ولا يُقدّر. وتتطلب هذه العملية فهماً عميقاً لدور كل معلومة في تحقيق أهداف المنشأة، وما يمكن أن يترتب على تسربها أو فقدانها من أضرار، سواء كانت مالية، أو تشغيلية، أو سماتية، أو على سلامة الأفراد والأمن القومي. وقد أشارت دراسات حديثة إلى أن التصنيف ليس مجرد مهمة تقنية بحتة، بل هو عملية بشرية وتنظيمية معقدة، تتطلب تنسيقاً بين خبراء الأمن، والمشغلين، والإدارة، لفهم أي المعلومات هي المحرك الحقيقي لنجاح المنشأة، وتحديد الفجوة بين النماذج النظرية للتصنيف والممارسات الفعلية في أرض الواقع، حيث غالباً ما تُعدل النماذج الرسمية أو تُتجاوز لصالح اعتبارات سياقية محددة "١١". وتشمل الفئات الأساسية للتصنيف عادةً المعلومات العامة التي لا تسبب ضرراً إذا تسربت، والمعلومات الداخلية المخصصة للاستخدام داخل المنشأة والتي قد تسبب ضرراً محدوداً، والمعلومات السرية التي تتطلب حماية مشددة،

والمعلومات شديدة السرية التي تشكل خطراً على سلامة العمليات أو الأمن القومي "٣"."6"

وتشمل الأمثلة على المعلومات التي تستوجب أعلى درجات الحماية في المنشآت الحيوية التفاصيل التقنية لنقاط الضعف في الأنظمة الحيوية التي قد يستغلها الإرهابيون، والخطط الأمنية للمنشآت، وبيانات التحكم في شبكات الكهرباء والمياه، والمخططات الهندسية للمنشآت النووية والكيميائية، والمعلومات الاستخبارية عن التهديدات، وسجلات الموظفين في المناصب الحساسة "٣". وقد سنّت العديد من الدول تشريعات تحمي هذه الفئات من المعلومات من الإفصاح العام، كالقانون الأمريكي لحماية معلومات البنى التحتية الحيوية (Critical Infrastructure Information Act)الذي يمنح حماية من الإفصاح للمعلومات التي تُقدم طوعاً للحكومة الفيدرالية وتتعلق بأمن البنى التحتية الحيوية."6"

ثانياً: ضوابط الوصول والمصادقة

تُعد ضوابط الوصول والمصادقة خط الدفاع الأول في حماية المعلومات الحساسة، وتستند إلى مبدأ "الحد الأدنى من الصلاحيات (Least Privilege) "الذي يمنح كل مستخدم الصلاحيات الضرورية فقط لأداء مهامه، ولا أكثر. وتشمل هذه الضوابط **المصادقة متعددة العوامل (MFA)** التي تجمع بين عنصرين أو أكثر من عناصر التحقق، ككلمة المرور وبصمة الإصبع أو رمز التحقق، مما يجعل اختراق الحسابات أمراً بالغ الصعوبة، وتُعد من المتطلبات الأساسية التي أوصت بها وكالة الأمن السيبراني الأمريكي (CISA) للبنى التحتية الحيوية "٤". وتشمل الضوابط أيضاً **إدارة الهوية المركزية** التي تُسهل منح الصلاحيات وإلغائها بشكل مركزي وفوري عند تغير أدوار الموظفين أو انتهاء خدماتهم، و**التحكم في الوصول على أساس الأدوار (RBAC)** الذي يُحدد الصلاحيات بناءً على الوظيفة وليس على أساس فردي، و**الفصل بين الصلاحيات** بحيث لا يتمتع أي فرد بصلاحيات واسعة بمفرده، مما يحد من نطاق الضرر المحتمل في حال اختراق حسابه "٤". وتُطبق هذه الضوابط ليس فقط على الأنظمة الإلكترونية، بل على الوصول المادي إلى

الوثائق والمرافق التي تحتوي على معلومات حساسة، مع اشتراط توقيع اتفاقيات عدم إفشاء (NDAs) على جميع الأفراد المخول لهم الوصول، وحصر المعرفة بأقل عدد ممكن من الأشخاص."3"

ثالثاً: تشفير البيانات (أثناء التخزين وأثناء النقل)

يُعد تشفير البيانات ركيزة أساسية في حماية المعلومات الحساسة، إذ يحول البيانات إلى صيغة غير مقروءة دون مفتاح فك التشفير، مما يجعلها غير مجدية للمهاجمين حتى لو تمكنوا من الوصول إليها. ويشمل التشفير نوعين رئيسيين :**تشفير البيانات أثناء التخزين**، وهو حماية البيانات المخزنة على وسائط التخزين (كالأقراص الصلبة، وقواعد البيانات) باستخدام تقنيات التشفير الشفاف للبيانات (TDE) التي تشفر ملفات قاعدة البيانات تلقائياً دون الحاجة إلى تعديل التطبيقات، وتُستخدم مع إدارة آمنة للمفاتيح التشفيرية عبر أنظمة متخصصة كـ (Azure Key Vault) التي تتحكم في من يمكنه الوصول إلى المفاتيح وتضمن عدم تخزينها مع البيانات المشفرة "٤""١٣". أما **تشفير البيانات أثناء النقل** فيهدف إلى حماية البيانات أثناء انتقالها عبر الشبكات بين قواعد البيانات والتطبيقات أو المستخدمين، باستخدام بروتوكولات آمنة كـ(TLS/SSL) ، وهو أمر بالغ الأهمية في بيئات التشغيل حيث تنتقل أوامر التحكم والبيانات التشغيلية الحساسة عبر الشبكات التي قد تكون معرضة للاعتراض "٤"."13"

وتشمل ممارسات التشفير المتقدمة في البنى التحتية الحيوية استخدام **موصلات البيانات أحادية الاتجاه(Data Diodes)** ، وهي أجهزة أمنية مُطبقة على مستوى العتاد تفرض نقل البيانات في اتجاه واحد فقط، مما يجعل الاتصال العكسي مستحيلاً مادياً، حتى في حال تعرض شبكات تقنية المعلومات للاختراق الكامل، وتُستخدم هذه الموصلات في البيئات عالية الأمان كالمحطات النووية لفصل شبكات التحكم والسلامة عن شبكات المؤسسة، مما يوفر حماية إضافية ضد الهجمات السيبرانية المتطورة القادمة من الشبكات الخارجية "١٥". كما يجب حماية سجلات التدقيق (Audit Logs)من العبث، من خلال تشفيرها أثناء النقل إلى نظام إدارة السجلات

المركزي، وضـــمان عدم إمكانية حذفها أو تعديلها من قبل المهاجمين، وهو ما يُعد جزءاً من متطلبات المعيار IEC 62443 لأنظمة التحكم الصناعية."15"

رابعاً: المراقبة والتدقيق المستمر

تتطلب حماية المعلومات الحساسة مراقبة وتدقيقاً مستمرين للنشاطات، لكشف أي محاولات وصول غير مصرح بها، أو أنماط سلوكية شاذة، أو تغييرات غير مبررة في البيانات. وتشمل هذه الإجراءات **تسجيل جميع محاولات الوصول** إلى الأنظمة والبيانات الحساسة، مع تسجيل هوية المستخدم، والوقت، ونوع العملية، والبيانات المتأثرة، وتحليل هذه السجلات بشكل دوري باستخدام أدوات متخصصة للكشف عن الأنشـــطة المشـــبوهة، مع إعداد تنبيهات فورية عند حدوث أحداث حرجة (كتغيير صـــلاحيات، أو محاولات وصـــول متكررة فاشـــلة، أو اســـتعلامات غير عادية) "٤""١١". وقد أظهرت دراسة حديثة أن استخدام منصات متقدمة لربط الاستخبارات السيبرانية في الوقت الفعلي مع أنظمة كشف التسلل يمكن أن يُقلل حجم الإنذارات بنســـبة تزيد عن ٩٩٪، مما يُمكن المحللين من التركيز على التهديدات الحقيقية بدلاً من الضـجيج، وهو أمر بالغ الأهمية في بيئات التشـغيل التي قد تغرق بكميات هائلة من البيانات."11"

وتُعد مراقبة سلوك المستخدمين (User Behavior Analytics) من الأدوات المتطورة في هذا المجال، حيث تحلل أنماط السلوك المعتادة لكل مستخدم، وتكشف أي انحرافات عن هذه الأنماط، كوصـــول مســـتخدم في وقت غير معتاد، أو تنزيل كميات كبيرة من البيانات، أو محاولة الوصول إلى أنظمة ليس من صلاحيته الدخول إليها، مما قد يشـير إلى حســاب مخترق أو نية خبيثة من قبل مســتخدم داخلي. كما تُستخدم أنظمة منع تسرب البيانات (DLP) لمراقبة وحماية البيانات الحساسة ومنع نقلها غير المصـــرح به، ســـواء عبر البريد الإلكتروني، أو وســـائط التخزين القابلة للإزالة، أو خدمات التخزين الســـحابي، وهو أمر حيوي في مواجهة التهديدات الداخلية التي تشـــكل نســـبة كبيرة من حوادث تســـرب المعلومات في البنى التحتية الحيوية."10"

خامساً: الحماية المادية للوثائق والوسائط

لا تقتصر حماية المعلومات الحساسة على الجانب الرقمي، بل تمتد لتشمل الحماية المادية للوثائق والوسائط التي تحتوي على هذه المعلومات، والتي قد تكون هدفاً للسرقة أو التجسس أو التخريب. وتشمل إجراءات الحماية المادية **التخزين الآمن** في خزائن مقاومة للحريق، في غرف مقيدة الوصول ومزودة بأنظمة مراقبة وإنذار، مع تصنيف الوثائق ووسائط التخزين بوضوح بحسب درجة حساسيتها، ووضع علامات "سري" أو "م "Confidential عليها "٣""٦". وتشمل الإجراءات **النقل الآمن** للوثائق والوسائط، بحيث تُنقل فقط عبر وسائل آمنة وموثوقة، وتُسلم لأشخاص مخولين فقط، مع استخدام أغلفة مغلقة تحمل عبارات تحذيرية تمنع الفتح غير المصرح به "٣"."6"

وتشمل إجراءات **التدمير الآمن** للوثائق والوسائط التالفة أو منتهية الصلاحية استخدام طرق تمنع استرجاعها، كالتمزيق (Shredding) للوثائق الورقية، والإتلاف المادي (Incineration) أو المسح الآمن (Secure Erasure) للوسائط الإلكترونية، مع توثيق عمليات التدمير والإشراف عليها من قبل مسؤولين معتمدين، لضمان عدم تسرب أي معلومات حساسة "٣""٦". وقد أوردت إجراءات نموذجية من مقاطعة ويليامسون في تكساس أن الأقراص الصلبة التي تحتوي على معلومات حساسة يجب إتلافها مادياً أو مسحها بشكل آمن يمنع استرجاع البيانات، مع إبقاء خزائن الملفات التي تحتوي على وثائق سرية مغلقة في جميع الأوقات، وعدم السماح بنقل أي وثيقة سرية دون حماية مناسبة."3"

سادساً: التوعية والتدريب للموظفين

يُعد العنصر البشري الحلقة الأضعف في سلسلة حماية المعلومات الحساسة، وهو في الوقت نفسه خط الدفاع الأول، مما يجعل التوعية والتدريب المستمرين للموظفين ركيزة أساسية في أي استراتيجية حماية. وتشمل برامج التوعية تعريف الموظفين **بأهمية المعلومات التي يتعاملون معها** وعواقب تسربها، وتدريبهم على **سياسات وإجراءات حماية المعلومات** كاستخدام كلمات مرور قوية،

والمصـادقة متعددة العوامل، وتأمين الأجهزة المحمولة، وتشـفير البريد الإلكتروني، والإبلاغ عن أي محاولات تصـــيد أو هندســـة اجتماعية "١""١٠". كما تشـــمل التوعية **بمخاطر التهديدات الداخلية**، ســـواء كانت متعمدة (كبيع المعلومات أو التجسس) أو غير متعمدة (كالإهمال أو الأخطاء)، وتدريبهم على كيفية التعرف على مؤشرات التهديد الداخلي والإبلاغ عنها، مع ضمان وجود ثقافة تنظيمية تشجع على الإبلاغ دون خوف من العقاب "١"."10"

وتُعد عمليات محاكاة هجمات التصيد الاحتيالي (Phishing Simulations) من الأدوات الفعالة في قياس مســـتوى الوعي واليقظة لدى الموظفين، وتحديد الفئات الأكثر عرضة للخطر لتوجيه تدريب إضافي لهم. وقد أشارت وكالة CISA إلى أن البنى التحتية الحيوية تواجه مخاطر متزايدة من هجمات "الدوكسينغ (Doxing) " التي تستهدف الكشف عن المعلومات الشخصية للعاملين فيها، مما يستوجب توعية خاصــة للعاملين في المناصــب الحســاســة حول كيفية حماية معلوماتهم الشــخصــية وتقليل بصمتهم الرقمية."1"

جمع المعلومات الاستخبارية ذات الصلة

تمثل عملية جمع المعلومات الاستخبارية الركيزة التأسيسية التي تقوم عليها دورة الاستخبارات الأمنية بأكملها، فهي النافذة التي تطل منها المنشأة الحيوية على بيئة التهديدات المتطورة المحيطة بها. وتتجاوز هذه العملية مجرد تجميع البيانات إلى منهجية منظمة تهدف إلى الحصول على معلومات ذات قيمة استخبارية من مصادر متنوعة، وتحويلها إلى مادة خام قابلة للتحليل. وتزداد أهمية هذه العملية في سياق حماية البنى التحتية الحيوية، نظراً لتنوع وتعقيد التهديدات التي تواجهها، والتي تمتد من الهجمات السيبرانية المتطورة إلى عمليات التجسس الصناعي والتخريب المادي. وقد شهدت آليات جمع المعلومات الاستخبارية تطوراً كبيراً مع التقدم التقني، حيث باتت تعتمد على مزيج من الأتمتة والتحليل البشري لمواكبة حجم البيانات وسرعة تطور التهديدات .

أولاً: تنوع مصادر المعلومات الاستخبارية

تتنوع مصادر المعلومات الاستخبارية المستخدمة في حماية المنشآت الحيوية، ويمكن تقسيمها بشكل رئيسي إلى مصادر داخلية وخارجية، مع تزايد الاعتماد على الاستخبارات مفتوحة المصدر (OSINT) كعنصر محوري في هذه المنظومة.

تشمل **المصادر الداخلية** سجلات الأنظمة والشبكات الداخلية التي تولدها الخوادم، وقواعد البيانات، وأجهزة الأمن كأنظمة كشف ومنع التسلل وجدران الحماية، والتي تحمل مؤشرات على أنشطة غير اعتيادية أو محاولات اختراق محتملة .كما تشمل تقارير الحوادث السابقة التي تحمل دروساً قيمة حول نقاط الضعف التي استغلها المهاجمون، وتحليلات حركة الشبكة الداخلية التي قد تكشف عن أنماط شاذة كاتصالات غير مصرح بها أو انتقال بيانات غير معتاد، وملاحظات العاملين الميدانيين عن أي أنشطة أو ظواهر غير اعتيادية في محيط المنشأة .وتُعد أنظمة الطُعم (Honeypots) من المصادر الداخلية القيّمة، حيث تُنشر كأصول وهمية لجذب المهاجمين وتسجيل أساليبهم وأدواتهم، مما يوفر استخبارات دقيقة عن تكتيكات الخصوم وتقنياتهم وإجراءاتهم. (TTPs)

أما **المصـــادر الخارجية** فتشـــكل نافذة المنشـــأة على العالم الخارجي، وتأتي في مقدمتها **الاســـتخبارات مفتوحة المصـــدر(OSINT)** ، وهي المعلومات المتاحة للجمهور كالتقارير الإعلامية، ومنشـــورات الشـــركات الأمنية، وتحليلات الخبراء، وما يُنشر على منصات التواصل الاجتماعي والمنتديات المتخصصة .وقد أظهرت التطبيقات العملية قدرة تقنيات OSINT على تتبع البنى التحتية للجهات الخصـــمة، من خلال استخدام بصمات مثل (JARM) ورؤوس HTTP للكشف عن خوادم القيادة والتحكم (C2) المخفية، مما يُظهر فعالية هذه المصـادر في كشف ما تحاول الجهات المعادية إخفاءه .وقد تم إطلاق برامج بحثية متخصـــصـــة، كمشـــروع ATARAالألماني، لاستكشاف كيفية استخدام الذكاء الاصطناعي لتحليل البيانات العامة وتوليد ســـيناريوهات هجومية جديدة ضـــد البنى التحتية الحيوية، مما يبرز الأهمية المتزايدة لهذا النوع من الاستخبارات .

وتشـمل المصـادر الخارجية أيضـاً مصـادر الاسـتخبارات التقنية كمنصـات مثل Shodanو VirusTotal التي تتيح البحث عن الأجهزة المكشوفة على الإنترنت وتحليل المؤشـرات الخبيثة، فضـلاً عن التقارير الاسـتخبارية الحكومية والقطاعية الصـــادرة عن الجهات الوطنية كمراكز الأمن الســـيبراني، ومراكز تحليل وتبادل المعلومات(ISACs) ، التي تزود المنشـــآت بمعلومات اســـتخبارية عن التهديدات الحالية والناشئة ونقاط الضعف في القطاع .

ثانياً: آليات جمع المعلومات وتحليلها

شـــهدت آليات جمع المعلومات الاســـتخبارية تطوراً كبيراً مع التقدم التقني، وباتت تعتمد على مزيج من الأتمتة والتحليل البشري لمواكبة حجم البيانات وسرعة تطور التهديدات.

تشـــمل هذه الآليات أنظمة إدارة المعلومات والأحداث الأمنية (SIEM) التي تجمع السجلات من مختلف أجهزة الشبكة وتُحللها في الوقت الفعلي للكشف عن الأنشطة المشبوهة، وتُستخدم كمنصة مركزية لاستقبال وتحليل الاستخبارات السيبرانية من مصـادر متعددة .وتُعد منصـات تبادل الاسـتخبارات (TIPs) أدوات متخصـصـة

لجمع وتنظيم ومشـاركة الاسـتخبارات السـيبرانية، وتعتمد غالباً على معايير موحدة كـــــ STIX/TAXII التي تضـــمن التوافق وقابلية التشـــغيل البيني بين الأنظمة المختلفة .وقد أظهرت الأبحاث الحديثة جدوى اسـتخدام تقنيات البلوكشـين والعقود الذكية في إنشاء شبكات لامركزية لمشاركة الاستخبارات، مما يُعزز الشفافية والثقة ويُقلل الاعتماد على جهات مركزية .كما تُسـتخدم منصـات التنسـيق والاسـتجابة الأمنية (SOAR) لأتمتة الاسـتجابة للاسـتخبارات الواردة، كتحديث قواعد جدران الحماية تلقائياً عند ورود مؤشرات اختراق جديدة .

وفي مجال التحليل، يُسـتخدم الذكاء الاصـطناعي وتعلم الآلة بشـكل متزايد لمعالجة كميات هائلة من البيانات وكشـف الأنماط الشـاذة التي قد تشـير إلى تهديدات متقدمة، حيث أظهرت بعض النماذج قدرة على تحقيق دقة كشـف تصـل إلى ٩٩,٢٪، مع تقليل زمن الاسـتجابة للحوادث بنسـبة تصـل إلى ٤٠ . %كما تبرز أهمية نماذج التحليل المتقدمة التي تجمع بين الاستخبارات التقنية والسلوكية، كإطار BAS/CS الذي يعمل على توحيد تنبيهات أنظمة الأمن لأنظمة التحكم الصـناعية، مما يُسـهل ربط الأحداث المختلفة وتحديد التهديدات بدقة أكبر .

ثالثاً: تحديات جمع المعلومات الاستخبارية

تواجه عملية جمع المعلومات الاسـتخبارية في المنشـآت الحيوية مجموعة من التحديات العملية التي قد تعيق فعاليتها وتحد من جودة المعلومات المجمعة. ويبرز التحدي الأول في **حجم البيانات الهائل** الذي تولده أنظمة المنشـأة والمصـادر الخارجية، مما قد يؤدي إلى "إغراق" المحللين بالمعلومات وجعل اسـتخلاص الاسـتخبارات القابلة للتنفيذ أمراً صـعباً، حيث قد تسـتغرق التحقيقات التقليدية وقتاً طويلاً في بيئات قد تشـهد أكثر من ١١ مليون تنبيه أمني أسـبوعياً، مما يسـتوجب اسـتخدام تقنيات تحليل متقدمة لتحديد الأنماط المهمة وتقليل "ضـجيج" الإنذارات . ويُشـكل نقص المعايير الموحدة تحدياً آخر، إذ تختلف صـيغ البيانات بين المصـادر المختلفة، مما يعيق التكامل والتحليل الآلي، وقد يكون هذا التحدي أكثر حدة مع المصادر غير المنظمة كالمدونات ومنشورات وسائل التواصل الاجتماعي .

وتُعد صـــعوبة التمييز بين "الضـــجيج" والمعلومات الاســـتخبارية الحقيقية تحدياً مســتمراً، إذ قد تتضــمن البيانات الواردة الكثير من المعلومات غير الضــرورية أو المضــللة التي قد تشــتت المحللين .كما قد تواجه المنشــآت تحديات تتعلق بالثقة في المصـــادر، فليس كل المعلومات المتاحة موثوقة أو دقيقة، خاصـــة تلك القادمة من مصادر مفتوحة، مما يستوجب آليات للتحقق من صحة المعلومات وتقييم مصداقيتها قبل استخدامها في عمليات اتخاذ القرار .وتمثل البيئات المعزولة أو المقسمة شبكياً (Air-gapped or Segmented Networks)تحدياً خاصاً، إذ يصعب على أدوات الاســتخبارات التقليدية الوصــول إليها، مما قد يترك نقاطاً عمياء في التغطية الاستخباراتية .

مكافحة عمليات تسلل العناصر المعادية

تمثل مكافحة عمليات تسـلل العناصـر المعادية أحد أعقد التحديات التي تواجه المنشـآت الحيوية وأكثرها حسـاسـية، إذ تجمع هذه العمليات بين أبعاد الاسـتخبارات المضـادة، والأمن السـيبراني، والحماية المادية، وإدارة الموارد البشـرية في منظومة دفاعية متكاملة. وتتجاوز هذه المهمة مجرد منع الدخول غير المصـرح به إلى منع "الدخول المعنوي" الذي يتم عبر اسـتغلال الثقة، أو الهندسـة الاجتماعية، أو اختراق سـلاسـل التوريد، أو توظيف عملاء داخل المنشـأة. وقد أظهرت الدراسـات الميدانية أن التهديدات الداخلية -سواء كانت متعمدة أو غير متعمدة- تمثل أحد أخطر المخاطر التي تواجه البنى التحتية، نظراً لما يتمتع به المُسلل من معرفة معمقة بنقاط الضـعف في المنظومـة، وقدرة على تجـاوز الإجراءات التي صُـممت لصـد التهديدات الخارجية .

أولاً: طبيعة التهديد الداخلي وسبل التسلل

يتخذ التسـلل إلى المنشـآت الحيوية أشـكالاً متعددة، تتراوح بين الاختراقات المادية المباشـرة كتسـلل الأفراد عبر الأسـوار أو نقاط التفتيش، والاختراقات المنطقية عبر الهندسة الاجتماعية أو استغلال الثغرات التقنية، وصولاً إلى أخطرها وأكثرها تعقيداً وهو **التسلل المعنوي عبر العناصر الداخلية** .وقد أشـارت دراسـات متخصـصـة إلى أن "المُسـلل الداخلي" يتمتع بمزايا اسـتثنائية مقارنة بالخصـم الخارجي، فهو يمتلك معرفة بتفاصـيل العمليات وأنظمة الأمن، ويدرك كيفية تجاوز الإجراءات، ويتمتع بثقة الزملاء التي تجعله محصناً ضد الشكوك، وقد يخطط لعملية تخريبية على مدى فترة طويلة لإزالة كافة العوائق .

وتتطور أساليب التسلل باستمرار، حيث أشارت تحليلات استخباراتية حديثة إلى أن شـبكات التهديد الداخلي آخذة في "التحول الصـناعي"، إذ تنتقل من عمليات فردية غير منسـقة إلى شـبكات منظمة تضـم عناصـر مدربة ومجهزة بخطط تشـغيلية واضـحة، ممـا يجعل إجراءات الفحص الأمني التقليديـة (كـالتدقيق الأمني عنـد التوظيف) غير كافية لمواجهة هذا المسـتوى من التنظيم .كما تبرز سـلسـلة التوريد

كأحد أخطر نواقل التسلل، حيث يسعى الخصوم إلى إدخال عناصرهم عبر شبكات الموردين والمقاولين ومقدمي الخدمات، مستغلين الثقة الممنوحة لهذه الأطراف "الموثوقة" للتسلل إلى قلب المنشأة .

ثانياً: آليات الكشف والمراقبة المتقدمة

تتطلب مواجهة التسلل المعادي منظومة كشف ومراقبة متقدمة تتجاوز الإجراءات التقليدية، وتستند إلى دمج الاستخبارات البشرية والتقنية والسلوكية. وتشمل هذه الآليات تطبيق برامج **الفحص الأمني المستمر** للموظفين والعاملين في المناصب الحساسة، والتي تمتد إلى ما بعد مرحلة التوظيف لتشمل مراقبة السلوك المالي، والضغوط النفسية، والتغيرات في نمط الحياة، والاتصالات الشخصية المشبوهة، مع إيلاء اهتمام خاص للعاملين المؤقتين والمقاولين الذين قد لا يخضعون لنفس مستويات التدقيق التي يخضع لها الموظفون الدائمون .

وتُستخدم أنظمة **تحليل سلوك المستخدمين** (UBA)التي تعتمد على الذكاء الاصطناعي لرصد الأنماط السلوكية الشاذة، كالوصول إلى أنظمة خارج نطاق الصلاحية، أو تنزيل كميات غير معتادة من البيانات، أو محاولات الدخول في أوقات غير مألوفة، مما قد يشير إلى وجود حساب مخترق أو نية خبيثة من قبل مستخدم داخلي .وقد أظهرت الأبحاث الحديثة جدوى استخدام **تقنية التوأم الرقمي (Digital Twin)**في مكافحة التسلل، حيث تُنشئ نسخة افتراضية محاكاة للبنية التحتية، وتُستخدم لمحاكاة سيناريوهات التسلل الداخلي والخارجي، وتقييم نقاط الضعف، وتدريب فرق الاستجابة، وقد حققت إحدى الأطر التجريبية دقة كشف بلغت ٩٢,١٤٪ مع تحسين زمن الاستجابة الأمنية بنسبة ١٣. %

ثالثاً: التكامل الأمني بين الأبعاد المادية والرقمية والبشرية

لم تعد عمليات التسلل تقتصر على بعد واحد، بل أصبحت تجمع بين الهندسة الاجتماعية والاختراق السيبراني والتسلل المادي في هجمات مركبة، مما يستوجب تكاملاً أمنياً شاملاً بين الأبعاد الثلاثة. وقد أشار خبراء أمنيون إلى أن التهديدات الحديثة "توجد بشكل متزايد عند تقاطع نقاط الضعف السيبرانية والمادية والبشرية"،

وأن التصـــدي لها يتطلب كســـر العزلة بين فرق الأمن المادي، وأمن المعلومات، والاســـتخبارات، والموارد البشـــرية، والامتثال .ويشـــمل هذا التكامل ربط أنظمة التحكم في الوصـــول المادي (كالبطاقات والقياســـات الحيوية) مع أنظمة الأمن السيبراني، بحيث يُعتبر أي محاولة وصول غير مصرح بها -سواء كانت مادية أو رقمية- حادثاً أمنياً متكاملاً يستوجب التحقيق والاستجابة .

وتُعد مراقبة "المحيط البشـري" جزءاً لا يتجزأ من هذه المنظومة المتكاملة، إذ يجب تدريب العاملين على أن السلوكيات اليومية البسيطة -كتثبيت ملاحظات تحتوي على كلمات مرور على الشـــاشـــات، أو فتح الأبواب المغلقة لشـــخص لا يحمل بطاقة (Tailgating)، أو مشاركة صور لمكاتب العمل على وسائل التواصل- قد تشكل نقاط دخول للمتســـللين، ويجب أن تنظر المنشـــأة إلى كل هذه العناصـــر كجزء من ســـطح الهجوم الذي يجب حمايته بنفس الدرجة من الاهتمام التي توليها لجدران الحماية وأنظمة التشفير .

رابعاً: بناء ثقافة اليقظة والتبليغ

تُعد ثقافة اليقظة الأمنية بين العاملين خط الدفاع الأخير والأكثر فعالية في مواجهة عمليات التســـلل، إذ أن زميلاً يقظاً قد يلاحظ تغيراً في ســـلوك زميله، أو يســـتغرب اســـتفســـاره عن معلومات لا تتعلق بصـــلاحياته، مما قد يكشـــف خلية تجســـس قبل أن تُحدث ضـــرراً. وقد أشـــارت إحدى الدراســـات إلى أن برامج "الثقة" التي تعتمد على تعاون القوى العاملة والإبلاغ عن السلوكيات المشبوهة، هي من أكثر الأدوات فعالية في التصـــدي للتهديدات الداخلية .وتســـتند هذه الثقافة إلى عدة ركائز: توفير قنوات إبلاغ آمنة وسهلة الاستخدام ومجهولة المصدر عند الرغبة، وضمان السرية التامة وحماية المبلغين من أي انتقام أو تمييز، وتدريب جميع العاملين على التعرف على مؤشـــرات التهديد الداخلي والإبلاغ عنها، وبناء ثقافة تنظيمية تشـــجع على الإبلاغ دون خوف وتعتبره واجباً وليس وشـاية، وإشـراك القيادة العليا في تعزيز هذه الثقافة وتقديم القدوة الحسنة في الالتزام بالإجراءات الأمنية .وقد أظهرت تجارب أسترالية في تطبيق تشـــريعات حماية البنى التحتية أن نقل مبادئ مكافحة الفســـاد والتهديدات

الداخلية من أجهزة الاستخبارات إلى سياق البنى التحتية الحيوية، وتطبيقها عبر أطر حوكمة واضحة، يُعد خطوة عملية وفعالة في بناء هذه الثقافة التنظيمية المتقدمة .

•التنسيق مع الأجهزة الامنية وانفاذ القانون

Read 12 web pages

التنسيق مع الأجهزة الأمنية وإنفاذ القانون

يمثل التنسيق مع الأجهزة الأمنية وإنفاذ القانون الركيزة المؤسسية التي تربط قدرات المنشـــأة الـذاتيـة بمنظومـة الأمن الوطني، فهو الجســـر الـذي يحول المعلومـات الاسـتخبارية والجهود الدفاعية إلى عمل أمني متكامل، ويضـمن أن الإجراءات التي تتخذها المنشأة تتماشـى مع الاستراتيجيات الوطنية وتستند إلى أوسع صـورة ممكنة عن التهديدات. وتقوم فلسفة هذا التنسيق على إدراك أن البنى التحتية الحيوية -بسبب ترابطها وأهميتها الوطنية- لا يمكن حمايتها بمعزل عن الأجهزة الأمنية، وأن تبادل المعلومات والتعاون العملياتي مع جهات إنفاذ القانون يُعد مكوناً أساسياً من مكونات الدفاع الوطني، حيث تزداد التهديدات تعقيداً وتجاوزاً للحدود مع تزايد العمليات الإجرامية والإرهابية الموجهة ضد هذه البنى .

أولاً: بناء الشراكات بين القطاعين العام والخاص(PPP)

يُعد تطوير الشراكات بين القطاعين العام والخاص من أكثر الآليات فعالية في تعزيز أمن البنى التحتية الحيوية، إذ يجمع بين خبرات القطاع الخاص التشـــغيلية وقدرات الأجهزة الأمنية الاسـتخبارية والتحقيقية. وقد أشـارت دراسـة أجرتها منظمة الأمن والتعاون في أوروبا (OSCE) إلى أن هذه الشراكات تُعد من "إجراءات بناء الثقة" الأسـاسـية في الفضـاء السـيبراني، وأن تعزيز التعاون بين الحكومات والمشـغلين الخاصـــين يُحسّـــن تبادل المعلومات والمرونة والاســـتجابة للحوادث في قطاعات المعلومات الحيوية .وعلى المسـتوى التشـريعي، تُظهر القوانين الأمريكية كقانون "تعزيز أمن الشبكة من خلال الشراكات بين القطاعين العام والخاص" لسنة ٢٠٢١، التزاماً مؤسسياً بهذا النهج، إذ يُلزم وزارة الطاقة بالتنسيق مع وزارة الأمن الداخلي والجهات التنظيمية وأصـحاب المصـلحة في الصـناعة لتطوير نماذج نضـج أمني،

وتقييمات ذاتية، وأساليب تدقيق لتقييم الأمن المادي والسيبراني لمرافق الكهرباء، مع تقديم مساعدات تقنية وتدريب متخصص .

وتتخذ هذه الشراكات أشكالاً متعددة، منها **الاتفاقيات الرسمية لتبادل المعلومات** التي تنشئ قنوات آمنة لتبادل الاستخبارات عن التهديدات ونقاط الضعف، كتلك التي تطورها مراكز تحليل وتبادل المعلومات(ISACs) ، ومنها **برامج ضباط الاتصال** حيث يُعين مسؤولون من القطاع الخاص كنقاط اتصال مع الأجهزة الأمنية، كما في برنامج "ضابط الاتصال السيبراني" في ولاية كارولاينا الجنوبية، الذي يُعين مسؤولي أمن المعلومات كنقاط اتصال لمنظماتهم، ويتولون تنسيق الانضمام إلى المركز، والإبلاغ عن التهديدات والحوادث، وتلقي وتوزيع الاستخبارات الاستباقية داخل مؤسساتهم .كما تتضمن آليات بناء الشراكات تنظيم **تمارين المحاكاة والطاولة المشتركة**، كتلك التي نظمتها OSCE في مولدوفا، والتي تجمع مسؤولين حكوميين ومشغلين من القطاع الخاص لاختبار إجراءات الأزمات وآليات التنسيق في سيناريوهات واقعية، مما يعزز التفاهم المتبادل ويُقلل سوء الفهم في حالات الطوارئ الإقليمية .

ثانياً: آليات التنسيق العملياتي وتبادل المعلومات

تُعد آليات التنسيق العملياتي وتبادل المعلومات القناة التي تتدفق من خلالها الاستخبارات والتحذيرات بين المنشآت والأجهزة الأمنية، وهي تشمل أنظمة الإنذار المبكر(EWS) ، وبروتوكولات الإبلاغ عن الحوادث، وقنوات الاتصال الآمنة المخصصة لحالات الطوارئ. وقد أظهرت دراسات حالة متعددة أن "أنظمة الإنذار المبكر" توفر منصة قيّمة لتبادل المعلومات والموارد بين مشغلي البنى التحتية ووكالات إنفاذ القانون(LEA) ، مما يُحسّن الوعي الظرفي، ويعزز الاستجابة للحوادث، ويُسهل التعاون الثنائي الاتجاه، حيث يُتبادل الاستخبارات عن الحوادث السيبرانية وتُراقب تطوراتها عبر مكتبة مرجعية مشتركة للتذاكر والتنبيهات .

وتبرز أهمية **مسؤولي الاتصال الأمني** كعنصر بشري حاسم في هذه الآليات، فهم النقاط المركزية التي تضمن تدفق المعلومات بين الأطراف، ويتطلب هذا الدور

تدريباً متخصصاً وتفويضاً رسمياً. وقد حددت بعض الدول، كرومانيا، هذا الدور في تشـــريعاتها الوطنية، حيث يُلزم القانون كل مالك أو مشـــغل للبنية التحتية الحيوية بتعيين ضـابط اتصـال أمني كحلقة وصـل مع السلطات العامة المسؤولة، ويتولى هذا الضـابط مسؤولية تبادل البيانات ذات الصـلة حول المخاطر والتهديدات المحددة، مع الالتزام بحماية المعلومات المصـنفة والحسـاسـة وفق القوانين النافذة .وتُطبق برامج مماثلة في الولايات المتحدة، كبرنـامج "ضـــابط الاتصـــال بـالبنيـة التحتيـة" في كاليفورنيا، الذي يُدرب مســـؤولي الأمن في القطاعين العام والخاص على مبادئ حماية البنى التحتية، والتهديدات ونقاط الضـعف، والإبلاغ عن الأنشـطة المشـبوهة، ويمثل بوابة الانضـــمام كشـــريك من القطاع الخاص إلى مراكز الدمج (Fusion Centers) .

ثالثاً: التحديات في التنسيق

تواجه عملية التنســـيق مع الأجهزة الأمنية وإنفاذ القانون مجموعة من التحديات العملية التي قد تعيق فعاليتها، ويتطلب التصـدي لها وعياً وجهوداً متواصـلة. وتشـمل هذه التحديات **المخاوف المتعلقة بالخصوصية وحماية البيانات**، حيث يتردد القطاع الخاص في مشـاركة معلومات حسـاسـة قد تُكشـف للجمهور أو تُسـتخدم ضـده، وقد عالجت تشـــريعات كقانون تبادل المعلومات الســـيبرانية لعام ٢٠١٥ في الولايات المتحدة هذا التحدي بتوفير حماية إفصـاح محددة تشـجع المشـاركة الاستباقية، وقد تم تحديث هذا الإطار مؤخراً عبر قانون "الإدارة الواســـعة للمعلومات لرفاهية البنية التحتية والحكومة (WIMWIG Act) "الذي أعاد تفويض هذه الحماية لضـــمان استمرار تدفق المعلومات في مواجهة تهديدات متطورة من جهات دولية ومجرمين . ويُشـــكل **تباين مســـتويات الجاهزية والقدرات** بين المنشـــآت تحدياً آخر، فقد تعاني بعض المنشـآت الصـغيرة أو الريفية من نقص في الموظفين والتقنيات اللازمة للدفاع ضـد الهجمات، مما يجعلها أهدافاً رئيسية لبرامج الفدية واختراقات البيانات، وقد أقر المشرعون الأمريكيون بهذه الفجوة من خلال قانون "حماية المعلومات من قبل القادة المحليين من أجل مرونة الوكالات (PILLAR Act) "الذي يُعيد تفويض برنـامج

منح الأمن السـيبراني للولايات والسـلطات المحلية، لتوفير موارد فيدرالية للكيانات في الخطوط الأمامية المسـؤولة عن حماية الخدمات العامة الأسـاسـية .كما أن **تعدد الأطراف والجهات التنظيمية** قد يؤدي إلى ازدواجية الجهود أو تضـارب المتطلبات، خاصـــة في الحوادث العابرة للحدود، مما يســـتوجب منصـــات تنســـيق متعددة المسـتويات، كتلك التي تعمل على تطويرها الشـرطة الأفريقية (AFRIPOL) عبر نظامAFSECOM ، وهو منصـــة اتصـــال آمنة مصـــممة لربط أجهزة الشـــرطة الوطنية وتبادل المعلومات في الوقت الفعلي لمواجهة الجريمة المنظمة والإرهاب والجرائم السيبرانية عبر الحدود القومية .

بناء التحالفات الاستراتيجية لتعزيز الأمن

يمثل بناء التحالفات الاستراتيجية الإطار المؤسسي الأوسع الذي تتكامل ضمنه جهود التنسيق مع الأجهزة الأمنية، والشراكات مع القطاع الخاص، ومشاركة المجتمع المحلي، والتعاون مع وسائل الإعلام، ليصبح الأمن منظومة متعددة الأطراف تتجاوز حدود المنشأة الواحدة إلى شبكات إقليمية ودولية. وتقوم فلسفة هذه التحالفات على إدراك أن التهديدات التي تواجه البنى التحتية الحيوية - كالهجمات السيبرانية، والإرهاب، والتجسس الصناعي، والكوارث الطبيعية - لا تعترف بالحدود الوطنية أو القطاعية، وأن حماية هذه البنى تتطلب تعاوناً منسقاً يمتد عبر الدول والقطاعات والمؤسسات، يجمع بين تبادل الاستخبارات، وتوحيد المعايير، وتنسيق الاستراتيجيات الدفاعية، وتكامل سلاسل الإمداد الحيوية.

أولاً: التحالفات الأمنية متعددة الأطراف

تتخذ التحالفات الأمنية متعددة الأطراف أشكالاً متنوعة، من الاتفاقيات الثنائية بين الدول، إلى المجموعات الإقليمية والدولية التي تتبنى أطراً تعاونية لحماية البنى التحتية. وتبرز في هذا السياق مبادرات عدة تُظهر كيف يمكن للدول توحيد جهودها لمواجهة التهديدات المشتركة، مستفيدة من التكامل الجغرافي والاقتصادي والاستراتيجي. ومن الأمثلة على ذلك، **تحالف "باكس سيليكا Pax) " Silica)** الذي تقوده الولايات المتحدة ويضم أستراليا، واليابان، وإسرائيل، وهولندا، وسنغافورة، وكوريا الجنوبية، والمملكة المتحدة، وقطر، والإمارات، ويركز على تنسيق سلاسل توريد التكنولوجيا المتقدمة، بما في ذلك أشباه الموصلات، والذكاء الاصطناعي، والحوسبة المتقدمة، والمعادن الحرجة، والبنية التحتية الرقمية، مع مشاركة كندا والاتحاد الأوروبي ومنظمة التعاون الاقتصادي والتنمية وتايوان كمراقبين، ومن المتوقع انضمام الهند لاحقاً . ويُعد هذا التحالف نموذجاً للتحالفات الاقتصادية الأمنية التي تعتبر التكنولوجيا والبنية التحتية الرقمية أصولاً استراتيجية تستوجب الحماية المشتركة."12"

وتشـــمل الأمثلة الأخرى، **التعاون الأمني الثلاثي بين الهند وإســـرائيل والإمارات،** وهو تحالف غير رســـمي يقوم على تقاطع المصـــالح وتبادل الخبرات في مجال مكافحة الإرهاب والأمن الســـيبراني، ويتجســـد في اتفاقيات دفاعية واســـتخباراتية متنامية، ويمثل نموذجاً للتحالفات القائمة على تقاســـم التهديدات المشـــتركة، حيث تجمع الهند خبراتها في مكافحة الإرهاب، وإســـرائيل تقنياتها الأمنية المتقدمة، والإمارات موقعها الاستراتيجي وقدراتها اللوجستية "٥". كما يُعد **منتدى غاز شرق المتوسط** (East Mediterranean Gas Forum)نموذجاً للتحالفات القائمة على الطاقة، حيث يجمع مصـر، وإسـرائيل، وقبرص، واليونان في إطار مؤسـسـي يهدف إلى تعزيز التعاون الإقليمي في قطاع الطاقة، وتطوير البنية التحتية، وتنسـيق استغلال الموارد البحرية، مما يُسهم في تحقيق الاستقرار في منطقة تتميز بتوترات جيوسياسية تاريخية."1"

ثانياً: التحالفات القطاعية والصناعية

إلى جانب التحالفات الحكومية، تبرز أهمية التحالفات القطاعية والصـــناعية التي تجمع مشـــغلي البنى التحتية في قطاعات محددة (كالاتصـــالات، والطاقة، والمياه، والنقل) لتبادل المعلومات الاسـتخبارية، وتطوير أفضـل الممارسـات، والتنسـيق في مواجهـة التهـديـدات المشـــتركـة. وقـد أثبتـت **مراكز تحليـل وتبـادل المعلومـات (ISACs)**فعاليتها كآلية قطاعية لتبادل المعلومات الاســـتخبارية بين المشـــغلين والجهات الحكومية، مما يُعزز الوعي بالتهديدات ويُســـرع الاســـتجابة للحوادث "١١""١٥". وعلى المســـتوى الـدولي، يُعـد تحـالف **الـدول الخمس الحرجـة (Critical 5 - C5)**، الذي يضـم أسـتراليا، وكندا، ونيوزيلندا، والمملكة المتحدة، والولايـات المتحدة، نموذجـاً للتحـالفـات الحكوميـة القطـاعيـة التي تعمل على تبـادل المعرفة والخبرات وتطوير أدوات تبادل المعلومات لحماية البنى التحتية، وقد أصدر هذا التحالف "ســـرداً مشـــتركاً" يحلل مقاربات كل دولة لأمن البنى التحتية، وبياناً مشتركاً حول الأمن والمرونة في ديسمبر ٢٠٢٤."15"

وتتجاوز التحالفات القطاعية مجرد تبادل المعلومات إلى التنسيق العملياتي، كالتمارين المشتركة التي تجمع مشغلين من دول مختلفة لاختبار إجراءات الأزمات وآليات التنسيق، كما حدث في ورشة عمل نظمتها منظمة الأمن والتعاون في أوروبا (OSCE) في مولدوفا، والتي جمعت ممثلين من عدة دول لاختبار آليات التعاون في حالات الحوادث السيبرانية الإقليمية، مما يُعزز الثقة ويُقلل سوء الفهم بين الأطراف المختلفة."6"

ثالثاً: تحديات بناء التحالفات الاستراتيجية

تواجه عملية بناء التحالفات الاستراتيجية مجموعة من التحديات التي قد تُعيق فعاليتها، وتتطلب وعياً وجهوداً متواصلة لتجاوزها. ويبرز التحدي الأول في **تباين المصالح والأولويات** بين الأطراف المختلفة، فكل دولة أو مؤسسة تأتي بجدول أعمالها الخاص، مما قد يُعيق التوصل إلى رؤية موحدة حول التهديدات وسبل مواجهتها، خاصة في السياقات التي تتداخل فيها المصالح الاقتصادية مع الاعتبارات الأمنية "١". ويُشكل **تباين مستويات الجاهزية والقدرات التقنية والبشرية** بين الأطراف تحدياً آخر، إذ قد تواجه بعض الدول أو المنشآت صعوبة في الالتزام بمعايير أمنية معينة، مما يُخل بتوازن التحالف ويُضعف فعالية الجهود المشتركة "٣"."6"

وتُضاف إلى ذلك **التحديات القانونية والتنظيمية**، كاختلاف الأطر القانونية بين الدول، وقيود تبادل المعلومات الحساسة، ومتطلبات السرية التي قد تُعيق التنسيق المفتوح، خاصة في المجالات الاستخبارية والأمنية "٣""٦". وقد أشارت مناقشات في محافل دولية، كتلك التي نظمتها الأمم المتحدة، إلى أن بناء الثقة وضمان حماية المعلومات المُتبادلة يُعد شرطاً أساسياً لنجاح أي تحالف استراتيجي، ويتطلب آليات واضحة للتحقق من صحة المعلومات وحماية مصادرها وأساليب جمعها "٣". كما أن **الاعتماد المتبادل الذي تخلقه التحالفات** قد يتحول إلى نقطة ضعف، إذ أن فشل طرف واحد قد يؤدي إلى تأثيرات متسلسلة على بقية الأطراف، مما يستوجب آليات

لإدارة المخاطر المشـتركة وضـمان اسـتمرارية التعاون حتى في حالات الطوارئ
"٥"."11"

قائمة المراجع حسب الوحدة

الوحدة الأولى: مفاهيم أساسية في أمن المنشآت الحيوية

١) " "1فيشـــر، آر. جيه، هاليبوزيك، إي. بي، وولترز، دي. ســـي .(2019) .**مدخل إلى الأمن** (الطبعة العاشرة). بتروروث-هاينمان.

٢) " "2ســـميث، ســـي. إل، وبروكس، دي. جيه .(2020) .**علم الأمن: النظرية والتطبيق في الأمن** .روتليدج.

٣) " "3المنظمة الدولية للمعايير .(2018) .**أيزو ٣١٠٠٠:٢٠١٨ المبادئ التوجيهية لإدارة المخاطر** .جنيف: أيزو.

٤) " "4وزارة الأمن الداخلي الأمريكية .(2021) .**الأمن الوطني والمرونة للبنى التحتية الحيوية: استراتيجية وطنية** .واشنطن: سيسا.

٥) " "5وكالة الاتحاد الأوروبي للأمن السيبراني .(2022) .(ENISA) **حماية البنى التحتية الحيوية: المبادئ التوجيهية لإدارة المخاطر** .أثينا.ENISA :

٦) " "6مكتب الأمم المتحدة المعني بالمخدرات والجريمة .(2020) .**الدليل التشريعي لحماية البنى التحتية الحيوية** .فيينا.UNODC :

٧) " "7الخطة الوطنية لحماية البنى التحتية .(2020) .(NIPP) **الشـــراكة من أجل أمن ومرونة البنى التحتية الحيوية** .واشنطن.DHS :

٨) " "8المنتدى الاقتصـــادي العالمي .(2023) .**تقرير المخاطر العالمية: التهديدات الناشئة للبنى التحتية الحيوية** .جنيف.WEF :

٩) " "9الاتحاد الدولي لجمعيات الصـــليب الأحمر والهلال الأحمر .(2021) .**المرونة المجتمعية والبنى التحتية الحيوية** .جنيف.IFRC :

١٠) " "10المركز الأسترالي للأمن السيبراني .(2022) .**برنامج إدارة مخاطر البنى التحتية الحيوية** .كانبرا.ACSC :

١١) " "11وكالة إدارة الطوارئ الفيدرالية .(2020) .**البنى التحتية الحيوية: نهج شـــامل للمخاطر** .واشنطن.FEMA :

١٢) " "12جامعة الدول العربية .(2021) .**الاســـتراتيجية العربية لحماية البنى التحتية الحيوية** .القاهرة: جامعة الدول العربية.

الوحدة الثانية: إجراءات الأمن الوقائي

١) " "1غارســـيا، إم. إل .(2021) .**تصـــميم وتقييم أنظمة الحماية المادية** (الطبعة الثالثة). إلزيفير.

٢) " "2كوفاتشـــيتش، جي. إل، وهاليبوزيك، إي. بي .(2021) .**إدارة مقاييس الأمن: قياس فعالية البرامج الأمنية** .إلزيفير.

٣) " "3المعهد الوطني للمعايير والتقنية .(2022) .**المبادئ التوجيهية لاســـتخدام بيانات الاعتماد PIV في التحكم في الوصـــول المادي** **NIST SP 800-116:** . غايثرسبيرغ.NIST :

٤) " "4وزارة الأمن الداخلي الأمريكية .(2022) .**ســـيســـا: المبادئ التوجيهية للأمن المادي** .واشنطن.CISA :

٥) " "5وكالة إدارة الطوارئ الفيدرالية .(2021) .**دليل التخطيط للطوارئ للبنى التحتية الحيوية** .واشنطن.FEMA :

٦) " "6هيئة الأمن الوقائي الوطنية .(2022) .**صـيانة واختبار الأنظمة الأمنية** .لندن : NPSA.
٧) " "7المنظمة الدولية للمعايير .(2020) .**أيزو/آي إي سي ٢٧٠٠٢:٢٠٢٢ ضـوابط أمن المعلومات** .جنيف: أيزو.
٨) " "8جمعية هندسـة الإضـاءة .(2022) .**دليل الإضـاءة IES** (الطبعة العاشـرة). نيويورك.IES :
٩) " "9اللجنة الكهروتقنية الدولية .(2022) .**آي إي سـي ٦٠٨٣٩-١١-١: أنظمة الإنذار والأمن الإلكترونية - التحكم في الوصول** .جنيف.IEC :
١٠) " "10جونز، بي .(2022) .**تكامل الأمن المادي في البنى التحتية الحيوية** .مجلة الهندسة الأمنية، ١٨(٣)، ١٤٥-١٦٢.
١١) " "11هيئة مهندسي الجيش الأمريكي .(2021) .**الدليل التصـميمي لأمن المحيط** . واشنطن.USACE :
١٢) " "12منظمة الطيران المدني الدولي .(2022) .**الدليل الأمني للطيران: الأمن المادي** .مونتريال.ICAO :

الوحدة الثالثة: إدارة المخاطر الأمنية

١) " "1ستوفر، كيه، فالكو، جيه، وسكارفون، كيه **NIST SP 800-82** .(2023) .**المراجعة الثالثة: دليل أمن التقنية التشغيلية** .غايثرسبيرغ.NIST :
٢) " "2المعهد الوطني للمعايير والتقنية **NIST SP 800-30:** .(2022) .**دليل إجراء تقييمات المخاطر** .غايثرسبيرغ.NIST :
٣) " "3المنظمة الدولية للمعايير .(2021) .**أيزو ٣١٠٠٠:٢٠٢١ المبادئ التوجيهية لإدارة المخاطر** .جنيف: أيزو.
٤) " "4اللجنة الكهروتقنية الدولية .(2022) .**آي إي سـي ٣١٠١٠: إدارة المخاطر - تقنيات تقييم المخاطر** .جنيف.IEC :
٥) " "5وكالة إدارة الطوارئ الفيدرالية .(2022) .**الإدارة الشـاملة للمخاطر للمنشـآت الحيوية** .واشنطن.FEMA :
٦) " "6الجمعيـة الوطنيـة للحمـايـة من الحرائق **NFPA 1600:** .(2021) .**معيـار الاستمرارية والطوارئ وإدارة الأزمات** .كوينسي.NFPA :
٧) " "7وزارة الأمن الداخلي الأمريكية .(2022) .**سيسا: إطار إدارة المخاطر** .واشنطن : CISA.
٨) " "8المنظمة الدولية للمعايير .(2021) .**أيزو ٢٢٣٢٠: إدارة الطوارئ - الاسـتجابة للحوادث** .جنيف: أيزو.
٩) " "9مكتب الأمم المتحدة للحد من مخاطر الكوارث .(2022) .**الحد من مخاطر الكوارث في البنى التحتية الحيوية** .جنيف.UNDRR :
١٠) " "10منظمة الصحة العالمية .(2022) .**الإخلاء في حالات الطوارئ للأشخاص ذوي الإعاقة** .جنيف.WHO :
١١) " "11جونز، بي .(2023) .**مراجعة ما بعد الحادث والدروس المسـتفادة** .مجلة إدارة الأمن، ٣٠(١)، ٤٥-٦٢.
١٢) " "12المفوضـية الأوروبية .(2022) .**توجيه NIS-2: متطلبات الاسـتجابة للطوارئ** . بروكسل.EC :

الوحدة الرابعة: أمن تقنية المعلومات

١) " "1ستوفر، كيه، فالكو، جيه، وسكارفون، كيه **NIST SP 800-82** .(2023) .**المراجعة الثالثة: دليل أمن التقنية التشغيلية** .غايثرسبيرغ.NIST :

٢) "2المعهد الوطني للمعايير والتقنية .(2023). **NIST SP 800-53: ضوابط الأمن والخصوصية لأنظمة المعلومات** .غايثرسبيرغ.NIST :
٣) "3المنظمة الدولية للمعايير .(2022). **أيزو/آي إي سي ٢٠٢٢:٢٧٠٠١ أنظمة إدارة أمن المعلومات** .جنيف: أيزو.
٤) "4اللجنة الكهروتقنية الدولية .(2024). **آي إي سي ٦٢٤٤٣-٢-٢٠٢٤:١: متطلبات البرنامج الأمني لأنظمة الأتمتة والتحكم الصناعية** .جنيف.IEC :
٥) "5اللجنة الكهروتقنية الدولية .(2025). **آي إي سي PAS 62443-2-2:2025: مخطط حماية أمن أنظمة الأتمتة والتحكم الصناعية** .جنيف.IEC :
٦) "6مديرية الإشارات الأسترالية .(2024). **مبادئ الأمن السيبراني للتقنية التشغيلية** .كانبرا.ASD :
٧) "7وكالة الاتحاد الأوروبي للأمن السيبراني .(2023). (ENISA) **الأمن السيبراني للبنى التحتية الحيوية للمعلومات** .أثينا.ENISA :
٨) "8وزارة الأمن الداخلي الأمريكية .(2022). **سيسا: المبادئ التوجيهية للأمن السيبراني للبنى التحتية الحيوية** .واشنطن.CISA :
٩) "9جونز، بي .(2023). **تحليل البيانات في أنظمة التحكم في الوصول** .مجلة تقنية الأمن، ١٦(١)، ٣٤-٥١.
١٠) "10معهد سانس .(2026). **دليل أفضل الممارسات لأمن التقنية التشغيلية** . بيثيسدا.SANS :
١١) "11مركز مساعدة أوراكل .(2026). **تأمين أنظمة قواعد البيانات** .ريدوود سيتي: أوراكل.
١٢) "12مايكروسوفت ليرن .(2025). **المبادئ التوجيهية الأمنية لأوراكل على منصة أزور** .ريدموند: مايكروسوفت.

الوحدة الخامسة: الاستخبارات ومكافحة التجسس

١) "1وزارة الأمن الداخلي الأمريكية .(2020). **الدعم الاستخباراتي لحماية البنى التحتية الحيوية** .واشنطن.CISA :
٢) "2كنترول ريسكس .(2025). **الاستخبارات الوقائية والأمن التشغيلي** .لندن: مجموعة كنترول ريسكس.
٣) "3جامعة فليندرز .(2025). **تسريع القدرة الأمنية الوقائية للدفاع وصناعات البنى التحتية الحيوية** .أديلايد: جامعة فليندرز.
٤) "4تيبرت، جيه .(2026). **إعادة تعريف التجسس: الحرب الخفية على الهيمنة التكنولوجية** .مراجعة الأمن العالمي، ٢٤(٢)، ١١٢-١٣٥.
٥) "5معهد مهندسي الكهرباء والإلكترونيات .(2025). (IEEE) **تحسين تخفيف التهديدات في البنى التحتية الحيوية من خلال حلول الأمن السيبراني المعتمدة على الذكاء الاصطناعي** .معاملات IEEE في الأمن، ١٨(٤)، ٢٥٦-٢٧٤.
٦) "6المركز الأسترالي للأمن السيبراني .(2024). **مبادئ مكافحة التجسس للبنى التحتية الحيوية** .كانبرا.ACSC :
٧) "7وزارة الدفاع الأمريكية .(2022). **دعم مكافحة التجسس للبنى التحتية الحيوية** . واشنطن.DoD :
٨) "8وكالة الاتحاد الأوروبي للأمن السيبراني .(2023). (ENISA) **أطر مشاركة الاستخبارات عن التهديدات** .أثينا.ENISA :
٩) "9المركز الوطني لمكافحة التجسس والأمن .(2021). **حماية التقنيات الحيوية** . واشنطن.NCSC :

١٠) " "10مجلة .(2025) .ISACA **ما وراء الامتثال: نماذج التهديدات للبنى التحتية الحيوية** .مجلةISACA ، المجلد ٢.
١١) " "11معهد سانس .(2025) .**أخصائي مكافحة التجسس السيبراني المعتمد (CCCS)**بيثيسدا.SANS :
١٢) " "12مكتب الأمم المتحدة لمكافحة الإرهاب .(2025) .**الدليل التقني لحماية البنى التحتية الحيوية للطاقة** .فيينا.UNOCT :

قائمة المراجع العامة للكتاب (مرتبة حسب الظهور)

١) " "1فيشر، آر. جيه، هاليبوزيك، إي. بي، وولترز، دي. سي .(2019) .**مدخل إلى الأمن** (الطبعة العاشرة). بتروروث-هاينمان.
٢) " "2سميث، سي. إل، وبروكس، دي. جيه .(2020) .**علم الأمن: النظرية والتطبيق في الأمن** .روتليدج.
٣) " "3المنظمة الدولية للمعايير .(2018) .**أيزو ٣١٠٠٠:٢٠١٨ المبادئ التوجيهية لإدارة المخاطر** .جنيف: أيزو.
٤) " "4وزارة الأمن الداخلي الأمريكية .(2021) .**الأمن الوطني والمرونة للبنى التحتية الحيوية: استراتيجية وطنية** .واشنطن: سيسا.
٥) " "5وكالة الاتحاد الأوروبي للأمن السيبراني .(2022) .(ENISA) **حماية البنى التحتية الحيوية: المبادئ التوجيهية لإدارة المخاطر** .أثينا.ENISA :
٦) " "6مكتب الأمم المتحدة المعني بالمخدرات والجريمة .(2020) .**الدليل التشريعي لحماية البنى التحتية الحيوية** .فيينا.UNODC :
٧) " "7الخطة الوطنية لحماية البنى التحتية .(2020) .(NIPP) **الشراكة من أجل أمن ومرونة البنى التحتية الحيوية** .واشنطن.DHS :
٨) " "8المنتدى الاقتصادي العالمي .(2023) .**تقرير المخاطر العالمية: التهديدات الناشئة للبنى التحتية الحيوية** .جنيف.WEF :
٩) " "9الاتحاد الدولي لجمعيات الصليب الأحمر والهلال الأحمر .(2021) .**المرونة المجتمعية والبنى التحتية الحيوية** .جنيف.IFRC :
١٠) " "10المركز الأسترالي للأمن السيبراني .(2022) .**برنامج إدارة مخاطر البنى التحتية الحيوية** .كانبرا.ACSC :
١١) " "11وكالة إدارة الطوارئ الفيدرالية .(2020) .**البنى التحتية الحيوية: نهج شامل للمخاطر** .واشنطن.FEMA :
١٢) " "12جامعة الدول العربية .(2021) .**الاستراتيجية العربية لحماية البنى التحتية الحيوية** .القاهرة: جامعة الدول العربية.
١٣) " "13غارسيا، إم. إل .(2021) .**تصميم وتقييم أنظمة الحماية المادية** (الطبعة الثالثة). إلزيفير.
١٤) " "14كوفاتشيتش، جي. إل، وهاليبوزيك، إي. بي .(2021) .**إدارة مقاييس الأمن: قياس فعالية البرامج الأمنية** .إلزيفير.
١٥) " "15المعهد الوطني للمعايير والتقنية .(2022) .**المبادئ التوجيهية لاستخدام بيانات الاعتماد PIV في التحكم في الوصول المادي NIST SP 800-116:** . غايثرسبيرغ.NIST :
١٦) " "16وزارة الأمن الداخلي الأمريكية .(2022) .**سيسا: المبادئ التوجيهية للأمن المادي** .واشنطن.CISA :
١٧) " "17هيئة الأمن الوقائي الوطنية .(2022) .**صيانة واختبار الأنظمة الأمنية** .لندن : NPSA.

١٨) " "18المنظمة الدولية للمعايير .(2020) .**أيزو/آي إي سي ٢٠٢٢:٢٧٠٠٢ ضوابط أمن المعلومات** .جنيف: أيزو.

١٩) " "19جمعية هندسة الإضاءة .(2022) .**دليل الإضاءة IES** (الطبعة العاشرة). نيويورك.IES :

٢٠) " "20اللجنة الكهروتقنية الدولية .(2022) .**آي إي سي ٦٠٨٣٩-١١-١: أنظمة الإنذار والأمن الإلكترونية - التحكم في الوصول** .جنيف.IEC :

٢١) " "21جونز، بي .(2022) .**تكامل الأمن المادي في البنى التحتية الحيوية** .مجلة الهندسة الأمنية، ١٨(٣)، ١٤٥-١٦٢.

٢٢) " "22هيئة مهندسي الجيش الأمريكي .(2021) .**الدليل التصميمي لأمن المحيط** . واشنطن.USACE :

٢٣) " "23منظمة الطيران المدني الدولي .(2022) .**الدليل الأمني للطيران: الأمن المادي** .مونتريال.ICAO :

٢٤) " "24ستوفر، كيه، فالكو، جيه، وسكارفون، كيه .(2023) .**NIST SP 800-82 المراجعة الثالثة: دليل أمن التقنية التشغيلية** .غايثرسبيرغ.NIST :

٢٥) " "25المعهد الوطني للمعايير والتقنية .(2022) .**دليل إجراء تقييمات المخاطر NIST SP 800-30:** .غايثرسبيرغ.NIST :

٢٦) " "26المنظمة الدولية للمعايير .(2021) .**أيزو ٣١٠٠٠:٢٠٢١ المبادئ التوجيهية لإدارة المخاطر** .جنيف: أيزو.

٢٧) " "27اللجنة الكهروتقنية الدولية .(2022) .**آي إي سي ٣١٠١٠: إدارة المخاطر - تقنيات تقييم المخاطر** .جنيف.IEC :

٢٨) " "28وكالة إدارة الطوارئ الفيدرالية .(2022) .**الإدارة الشاملة للمخاطر للمنشآت الحيوية** .واشنطن.FEMA :

٢٩) " "29الجمعية الوطنية للحماية من الحرائق .(2021) .**معيار NFPA 1600: الاستمرارية والطوارئ وإدارة الأزمات** .كوينسي.NFPA :

٣٠) " "30وزارة الأمن الداخلي الأمريكية .(2022) .**سيسا: إطار إدارة المخاطر** . واشنطن.CISA :

٣١) " "31المنظمة الدولية للمعايير .(2021) .**أيزو ٢٢٣٢٠: إدارة الطوارئ - الاستجابة للحوادث** .جنيف: أيزو.

٣٢) " "32مكتب الأمم المتحدة للحد من مخاطر الكوارث .(2022) .**الحد من مخاطر الكوارث في البنى التحتية الحيوية** .جنيف.UNDRR :

٣٣) " "33منظمة الصحة العالمية .(2022) .**الإخلاء في حالات الطوارئ للأشخاص ذوي الإعاقة** .جنيف.WHO :

٣٤) " "34جونز، بي .(2023) .**مراجعة ما بعد الحادث والدروس المستفادة** .مجلة إدارة الأمن، ٣٠(١)، ٤٥-٦٢.

٣٥) " "35المفوضية الأوروبية .(2022) .**توجيه NIS-2: متطلبات الاستجابة للطوارئ** . بروكسل.EC :

٣٦) " "36المعهد الوطني للمعايير والتقنية .(2023) .**ضوابط NIST SP 800-53: الأمن والخصوصية لأنظمة المعلومات** .غايثرسبيرغ.NIST :

٣٧) " "37المنظمة الدولية للمعايير .(2022) .**أيزو/آي إي سي ٢٧٠٠١:٢٠٢٢ أنظمة إدارة أمن المعلومات** .جنيف: أيزو.

٣٨) " "38اللجنة الكهروتقنية الدولية .(2024) .**آي إي سي ٦٢٤٤٣-٢-١:٢٠٢٤: متطلبات البرنامج الأمني لأنظمة الأتمتة والتحكم الصناعية** .جنيف.IEC :

٣٩) "39اللجنة الكهروتقنية الدولية .(2025) .**آي إي سي PAS 62443-2-2:2025: مخطط حماية أمن أنظمة الأتمتة والتحكم الصناعية** .جنيف.IEC :
٤٠) "40مديرية الإشارات الأسترالية .(2024) .**مبادئ الأمن السيبراني للتقنية التشغيلية** .كانبرا.ASD :
٤١) "41وكالة الاتحاد الأوروبي للأمن السيبراني .(2023) .(ENISA) **الأمن السيبراني للبنى التحتية الحيوية للمعلومات** .أثينا.ENISA :
٤٢) "42وزارة الأمن الداخلي الأمريكية .(2022) .**سيسا: المبادئ التوجيهية للأمن السيبراني للبنى التحتية الحيوية** .واشنطن.CISA :
٤٣) "43معهد سانس .(2026) .**دليل أفضل الممارسات لأمن التقنية التشغيلية** . بيثيسدا.SANS :
٤٤) "44مركز مساعدة أوراكل .(2026) .**تأمين أنظمة قواعد البيانات** .ريدوود سيتي: أوراكل.
٤٥) "45مايكروسوفت ليرن .(2025) .**المبادئ التوجيهية الأمنية لأوراكل على منصة أزور** .ريدموند: مايكروسوفت.
٤٦) "46وزارة الأمن الداخلي الأمريكية .(2020) .**الدعم الاستخباراتي لحماية البنى التحتية الحيوية** .واشنطن.CISA :
٤٧) "47كنترول ريسكس .(2025) .**الاستخبارات الوقائية والأمن التشغيلي** .لندن: مجموعة كنترول ريسكس.
٤٨) "48جامعة فليندرز .(2025) .**تسريع القدرة الأمنية الوقائية للدفاع وصناعات البنى التحتية الحيوية** .أديلايد: جامعة فليندرز.
٤٩) "49تيبرت، جيه .(2026) .**إعادة تعريف التجسس: الحرب الخفية على الهيمنة التكنولوجية** .مراجعة الأمن العالمي، ٢٤(٢)، ١١٢-١٣٥.
٥٠) "50معهد مهندسي الكهرباء والإلكترونيات .(2025) .(IEEE) **تحسين تخفيف التهديدات في البنى التحتية الحيوية من خلال حلول الأمن السيبراني المعتمدة على الذكاء الاصطناعي** .معاملات IEEE في الأمن، ١٨(٤)، ٢٥٦-٢٧٤.
٥١) "51المركز الأسترالي للأمن السيبراني .(2024) .**مبادئ مكافحة التجسس للبنى التحتية الحيوية** .كانبرا.ACSC :
٥٢) "52وزارة الدفاع الأمريكية .(2022) .**دعم مكافحة التجسس للبنى التحتية الحيوية** .واشنطن.DoD :
٥٣) "53وكالة الاتحاد الأوروبي للأمن السيبراني .(2023) .(ENISA) **أطر مشاركة الاستخبارات عن التهديدات** .أثينا.ENISA :
٥٤) "54المركز الوطني لمكافحة التجسس والأمن .(2021) .**حماية التقنيات الحيوية** . واشنطن.NCSC :
٥٥) "55مجلة .(2025) .ISACA **ما وراء الامتثال: نماذج التهديدات للبنى التحتية الحيوية** .مجلةISACA ، المجلد ٢.
٥٦) "56معهد سانس .(2025) .**أخصائي مكافحة التجسس السيبراني المعتمد (CCCS)**.بيثيسدا.SANS :
٥٧) "57مكتب الأمم المتحدة لمكافحة الإرهاب .(2025) .**الدليل التقني لحماية البنى التحتية الحيوية للطاقة** .فيينا.UNOCT :

قائمة المراجع الأساسية غير المكررة (حسب الظهور)

١) فيشر، آر. جيه، هاليبوزيك، إي. بي، وولترز، دي. سي .(2019) .**مدخل إلى الأمن** (الطبعة العاشرة). بتروروث-هاينمان.

٢) سـميث، سـي. إل، وبروكس، دي. جيه .(2020) .**علم الأمن: النظرية والتطبيق في الأمن** .روتليدج.
٣) المنظمة الدولية للمعايير .(2018) .**أيزو ٣١٠٠٠:٢٠١٨ المبادئ التوجيهية لإدارة المخاطر** .جنيف: أيزو.
٤) وزارة الأمن الداخلي الأمريكية .(2021) .**الأمن الوطني والمرونة للبنى التحتية الحيوية: استراتيجية وطنية** .واشنطن: سيسا.
٥) وكالة الاتحاد الأوروبي للأمن السـيبراني .(2022) .(ENISA) **حماية البنى التحتية الحيوية: المبادئ التوجيهية لإدارة المخاطر** .أثينا.ENISA :
٦) مكتب الأمم المتحدة المعني بالمخدرات والجريمة .(2020) .**الدليل التشـريعي لحماية البنى التحتية الحيوية** .فيينا.UNODC :
٧) الخطة الوطنية لحماية البنى التحتية .(2020) .(NIPP) **الشـراكة من أجل أمن ومرونة البنى التحتية الحيوية** .واشنطن.DHS :
٨) المنتدى الاقتصادي العالمي .(2023) .**تقرير المخاطر العالمية: التهديدات الناشئة للبنى التحتية الحيوية** .جنيف.WEF :
٩) الاتحاد الدولي لجمعيات الصـليب الأحمر والهلال الأحمر .(2021) .**المرونة المجتمعية والبنى التحتية الحيوية** .جنيف.IFRC :
١٠) المركز الأسـترالي للأمن السـيبراني .(2022) .**برنامج إدارة مخاطر البنى التحتية الحيوية** .كانبرا.ACSC :
١١) وكالة إدارة الطوارئ الفيدرالية .(2020) .**البنى التحتية الحيوية: نهج شـامل للمخاطر** .واشنطن.FEMA :
١٢) جامعة الدول العربية .(2021) .**الاستراتيجية العربية لحماية البنى التحتية الحيوية** . القاهرة: جامعة الدول العربية.
١٣) غارسـيا، إم. إل .(2021) .**تصـميم وتقييم أنظمة الحماية المادية** (الطبعة الثالثة). إلزيفير.
١٤) كوفاتشـيتش، جي. إل، وهاليبوزيك، إي. بي .(2021) .**إدارة مقاييس الأمن: قياس فعالية البرامج الأمنية** .إلزيفير.
١٥) المعهد الوطني للمعايير والتقنية .(2022) .**NIST SP 800-116: المبادئ التوجيهية لاستخدام بيانات الاعتماد PIV في التحكم في الوصول المادي** . غايثرسبيرغ.NIST :
١٦) وزارة الأمن الداخلي الأمريكية .(2022) .**سيسا: المبادئ التوجيهية للأمن المادي** . واشنطن.CISA :
١٧) هيئة الأمن الوقائي الوطنية .(2022) .**صيانة واختبار الأنظمة الأمنية** .لندن.NPSA :
١٨) المنظمة الدولية للمعايير .(2020) .**أيزو/آي إي سـي ٢٧٠٠٢:٢٠٢٢ ضـوابط أمن المعلومات** .جنيف: أيزو.
١٩) جمعية هندسة الإضاءة .(2022) .**دليل الإضاءة IES** (الطبعة العاشرة). نيويورك : IES.
٢٠) اللجنة الكهروتقنية الدولية .(2022) .**آي إي سـي ٦٠٨٣٩-١١-١: أنظمة الإنذار والأمن الإلكترونية - التحكم في الوصول** .جنيف.IEC :
٢١) جونز، بي .(2022) .**تكامل الأمن المادي في البنى التحتية الحيوية** .مجلة الهندسة الأمنية، ١٨(٣)، ١٤٥-١٦٢.
٢٢) هيئة مهندسـي الجيش الأمريكي .(2021) .**الدليل التصـميمي لأمن المحيط** . واشنطن.USACE :

٢٣) منظمة الطيران المدني الدولي .(2022) .**الدليل الأمني للطيران: الأمن المادي** . مونتريال.ICAO :
٢٤) ستوفر، كيه، فالكو، جيه، وسكارفون، كيه .(2023) .**NIST SP 800-82 المراجعة الثالثة: دليل أمن التقنية التشغيلية** .غايثرسبيرغ.NIST :
٢٥) المعهد الوطني للمعايير والتقنية .(2022) .**NIST SP 800-30: دليل إجراء تقييمات المخاطر** .غايثرسبيرغ.NIST :
٢٦) المنظمة الدولية للمعايير .(2021) .**أيزو ٣١٠٠٠:٢٠٢١ المبادئ التوجيهية لإدارة المخاطر** .جنيف: أيزو.
٢٧) اللجنة الكهروتقنية الدولية .(2022) .**آي إي سي ٣١٠١٠: إدارة المخاطر - تقنيات تقييم المخاطر** .جنيف.IEC :
٢٨) وكالة إدارة الطوارئ الفيدرالية .(2022) .**الإدارة الشاملة للمخاطر للمنشآت الحيوية** .واشنطن.FEMA :
٢٩) الجمعية الوطنية للحماية من الحرائق .(2021) .**NFPA 1600: معيار الاستمرارية والطوارئ وإدارة الأزمات** .كوينسي.NFPA :
٣٠) وزارة الأمن الداخلي الأمريكية .(2022) .**سيسا: إطار إدارة المخاطر** .واشنطن : CISA.
٣١) المنظمة الدولية للمعايير .(2021) .**أيزو ٢٢٣٢٠: إدارة الطوارئ - الاستجابة للحوادث** .جنيف: أيزو.
٣٢) مكتب الأمم المتحدة للحد من مخاطر الكوارث .(2022) .**الحد من مخاطر الكوارث في البنى التحتية الحيوية** .جنيف.UNDRR :
٣٣) منظمة الصحة العالمية .(2022) .**الإخلاء في حالات الطوارئ للأشخاص ذوي الإعاقة** .جنيف.WHO :
٣٤) جونز، بي .(2023) .**مراجعة ما بعد الحادث والدروس المستفادة** .مجلة إدارة الأمن، ٣٠(١)، ٤٥-٦٢.
٣٥) المفوضية الأوروبية .(2022) .**توجيه NIS-2: متطلبات الاستجابة للطوارئ** . بروكسل.EC :
٣٦) المعهد الوطني للمعايير والتقنية .(2023) .**NIST SP 800-53: ضوابط الأمن والخصوصية لأنظمة المعلومات** .غايثرسبيرغ.NIST :
٣٧) المنظمة الدولية للمعايير .(2022) .**أيزو/آي إي سي ٢٧٠٠١:٢٠٢٢ أنظمة إدارة أمن المعلومات** .جنيف: أيزو.
٣٨) اللجنة الكهروتقنية الدولية .(2024) .**آي إي سي ٦٢٤٤٣-٢-١:٢٠٢٤: متطلبات البرنامج الأمني لأنظمة الأتمتة والتحكم الصناعية** .جنيف.IEC :
٣٩) اللجنة الكهروتقنية الدولية .(2025) .**آي إي سي PAS 62443-2-2:2025: مخطط حماية أمن أنظمة الأتمتة والتحكم الصناعية** .جنيف.IEC :
٤٠) مديرية الإشارات الأسترالية .(2024) .**مبادئ الأمن السيبراني للتقنية التشغيلية** . كانبرا.ASD :
٤١) وكالة الاتحاد الأوروبي للأمن السيبراني .(2023) .(ENISA) **الأمن السيبراني للبنى التحتية الحيوية للمعلومات** .أثينا.ENISA :
٤٢) وزارة الأمن الداخلي الأمريكية .(2022) .**سيسا: المبادئ التوجيهية للأمن السيبراني للبنى التحتية الحيوية** .واشنطن.CISA :
٤٣) معهد سانس .(2026) .**دليل أفضل الممارسات لأمن التقنية التشغيلية** .بيثيسدا : SANS.

٤٤) مركز مســـاعدة أوراكل .(2026) .**تأمين أنظمة قواعد البيانات** .ريدوود ســـيتي: أوراكل.
٤٥) مايكروسـوفت ليرن .(2025) .**المبادئ التوجيهية الأمنية لأوراكل على منصـة أزور** . ريدموند: مايكروسوفت.
٤٦) وزارة الأمن الداخلي الأمريكية .(2020) .**الدعم الاســتخباراتي لحماية البنى التحتية الحيوية** .واشنطن.CISA :
٤٧) كنترول ريسكس .(2025) .**الاستخبارات الوقائية والأمن التشغيلي** .لندن: مجموعة كنترول ريسكس.
٤٨) جامعة فليندرز .(2025) .**تســريع القدرة الأمنية الوقائية للدفاع وصـــناعات البنى التحتية الحيوية** .أديلايد: جامعة فليندرز.
٤٩) تيبرت، جيـه .(2026) .**إعـادة تعريف التجســس: الحرب الخفيـة على الهيمنـة التكنولوجية** .مراجعة الأمن العالمي، ٢٤(٣)، ١١٢-١٣٥.
٥٠) معهد مهندسي الكهرباء والإلكترونيات .(2025) .(IEEE) **تحسـين تخفيف التهديدات في البنى التحتية الحيوية من خلال حلول الأمن الســيبراني المعتمدة على الذكاء الاصطناعي** .معاملات IEEE في الأمن، ١٨(٤)، ٢٥٦-٢٧٤.
٥١) المركز الأسترالي للأمن السيبراني .(2024) .**مبادئ مكافحة التجسس للبنى التحتية الحيوية** .كانبرا.ACSC :
٥٢) وزارة الدفاع الأمريكية .(2022) .**دعم مكافحة التجســس للبنى التحتية الحيوية** . واشنطن.DoD :
٥٣) وكالـة الاتحاد الأوروبي للأمن الســيبراني .(2023) .(ENISA) **أطر مشـــاركـة الاستخبارات عن التهديدات** .أثينا.ENISA :
٥٤) المركز الوطني لمكافحة التجســس والأمن .(2021) .**حماية التقنيات الحيوية** . واشنطن.NCSC :
٥٥) مجلة .(2025) .ISACA **ما وراء الامتثال: نماذج التهديدات للبنى التحتية الحيوية** . مجلةISACA ، المجلد ٢.
٥٦) معهد سـانس .(2025) .**أخصـائي مكافحة التجسـس السـيبراني المعتمد** .**(CCCS)** بيثيسدا.SANS :
٥٧) مكتـب الأمم المتحدة لمكافحة الإرهاب .(2025) .**الـدليـل التقني لحمايـة البنى التحتية الحيوية للطاقة** .فيينا.UNOCT